

CAESAR8: an agile enterprise architecture approach to managing information security risks in business change projects

Paul James Loft

**Faculty of Computing, Engineering and
Media**

December 2021

**A thesis submitted in fulfilment of the University's
requirements for the Degree of Doctor of Philosophy**



Declaration

To the best of my knowledge I confirm that the work in this thesis is my original work undertaken for the degree of AWARD in the Faculty of CEM, De Montfort University. I confirm that no material of this thesis has been submitted for any other degree or qualification at any other university. I also declare that parts of this thesis have been submitted for publications.

Abstract

Implementing an Enterprise Architecture (EA) should enable organizations to increase the accuracy of information security risk assessments. Studies show that EAs provide an holistic perspective that improves information security risk management (ISRM). However, many organizations have been unable or unwilling to fully implement EA frameworks. The requirements for implementation of an EA can be unclear, the full benefits of many commercial frameworks is uncertain and the overheads of creating and maintaining EA artifacts considered unacceptable, especially for organizations following agile business change programs or having limited resource.

Following the Design Science Research methodology, this thesis describes a comprehensive and multidisciplinary approach to design a new model that can be used for the dynamic and holistic reviews of information security risks in business change projects. The model incorporates five novel design principles that are independent of any existing EA framework, security standard or maturity model. This new model is called CAESAR8 - Continuous Agile Enterprise Security Architecture Review in 8 domains.

CAESAR8 incorporates key ISRM success factors that have been determined from root cause analysis of information security failures. Combining systems thinking with agile values and lean concepts into the design has ensured that the impact of a change is considered holistically and continuously, prioritizing the EA process over the creation of EA artifacts. Inclusion of human behavioral-science has allowed the capture of diverse and often tacit knowledge held by different stakeholders impacted by a business change, whilst avoiding the dangers of groupthink. CAESAR8's presentation of the results provides an impactful and easy-to-interpret metric that is designed to be shared with senior business executives to improve intervention decisions.

This thesis demonstrates how CAESAR8 has been developed into a working prototype and presents case studies that describe the model in operation. A diverse group of experts were given access to a working IT prototype for a hands-on evaluation of CAESAR8. An analysis of their findings confirms the model's novel scientific contribution to ISRM.

Acknowledgements

I would like to give thanks to my supervisors: Prof. Helge Janicke, Dr Isabel Wagner, Dr Ying He and Dr Iryna Yevseyeva. Thank you for steering me through my studies, giving your time and patience in reviewing drafts and offering your invaluable advice.

Thank you to Mark Brett, for encouraging me to do this research and helping me to get started. Thank you to all of those who have participated in my research. I am grateful your commitment in time and expertise to my study.

And finally, a special thank you to my wife, Anne, for your endless support and encouragement. You have helped me through every step of this long and challenging journey. Thank you for your understanding and for the sacrifices that you have made to support me over the past years. Your contribution to my research could never be overstated.

Contents

Abstract	ii
Acknowledgements	iii
1 Introduction	1
1.1 The theoretical benefits of EA/EISA	1
1.2 The practical problems for EA/EISA	3
1.3 Motivation behind my research	6
1.4 Research aim	8
1.5 Research questions	9
1.6 Research contribution	10
1.6.1 Designing a practical solution that suits agile projects .	11
1.6.2 Designing a practical solution that suits the smaller business	13
1.6.3 A shared architecture concept	14
1.7 Structure of thesis	14
1.8 Conclusion of Introduction	16
2 Literature Review	17
2.1 Search plan	17
2.2 Performance of information security risk management	18
2.2.1 Applying the Systematic Literature Review methodology	19
2.2.1.1 Inclusion criteria	19
2.2.1.2 Exclusion criteria	20
2.2.1.3 Search keywords	20

2.2.1.4	Search strings	21
2.2.1.5	Search results	23
2.2.1.6	Analysis method	24
2.2.2	Performance of information security expressed in the context of the 6Ws categorization	27
2.2.2.1	WHY Nodes	33
2.2.2.2	WHEN Nodes	38
2.2.2.3	WHO Nodes	40
2.2.2.4	WHAT Nodes	51
2.2.2.5	WHERE Nodes	56
2.2.2.6	HOW Nodes	57
2.2.3	Performance of Enterprise Architecture	60
2.2.4	Difference between Private and Public Sectors	62
2.2.4.1	Security challenges for the Public Sector	63
2.2.4.2	Security Challenges for the Private Sector	64
2.3	Exploratory literature review	65
2.3.1	Systems Thinking	66
2.3.2	The use of checklists	67
2.3.3	Agile and Lean Concepts	68
2.3.3.1	Agile	68
2.3.3.2	Lean	70
2.3.4	Cognitive Diversity	72
2.3.5	Groupthink	75
2.3.6	Metrics and visualization	75
2.3.7	Security cultures	79
2.4	Search for similar artifacts	81
2.4.1	Explanation of search results	82
2.4.2	Discussion on the SAFE model	83
2.4.3	Discussion on PFIREs	85
2.4.4	Theories for the EA discipline	86
2.5	Conclusion of Literature Review	89

3	Research Methodology	91
3.1	Design Science Research Approach	91
3.2	Design Science Research Process Overview	93
3.2.1	Step 1: Problem Identification	95
3.2.2	Step 2: Objective of the Artifact	95
3.2.3	Step 3: Design and Development	96
3.2.4	Step 4: Demonstration	96
3.2.5	Step 5: Evaluation	97
3.2.6	Step 6: Communication	101
3.3	Conclusion of Research Methodology	102
4	Problem identification and objectives	103
4.1	Problem identification	103
4.1.1	Fifteen common business problem areas for informa- tion security management	104
4.1.2	Underlying issues for security strategies	105
4.2	Objectives	106
4.2.1	Addressing known problems and underlying issues . . .	106
4.2.2	Agile and Lean	107
4.2.3	Additional design information	107
4.2.4	Design Goals for CAESAR8	108
4.2.5	How the design goals address the identified problems .	111
4.3	Conclusion of Problem Identification and Objectives	113
5	Root cause analysis of IS performance to inform CAESAR8 design	114
5.1	Quantitative analysis of the coding	114
5.2	Qualitative analysis for node domains	117
5.2.1	Information Assets	121
5.2.2	External Factors	122
5.2.3	Technology Infrastructure	123
5.2.4	Business Process	124
5.2.5	Enterprise Architecture	125

5.2.6	Security Governance	126
5.2.7	Management Influence	128
5.2.8	Human Factors	129
5.3	Pairwise analysis of strongest node correlations	130
5.4	5 Maturity Levels	135
5.5	Performance Markers	138
5.5.1	Answering the performance marker questions	140
5.5.2	Presentation of CAESAR8 results	141
5.6	Conclusion of Root Cause Analysis	142
6	CAESAR8 design and development	144
6.1	Final CAESAR8 model design principles	147
6.1.1	Principle 1: Base model on a practical, holistic design.	147
6.1.2	Principle 2: Gather multiple stakeholder perspectives.	147
6.1.3	Principle 3: Unify around a tractable checklist.	148
6.1.4	Principle 4: Value process over EA artifacts.	148
6.1.5	Principle 5: Provide a collective visualization.	148
6.2	Ensuring all business departments' perspectives are represented	149
6.2.1	Supporting self-assessments for multiple stakeholders	149
6.2.1.1	<i>Trust</i> other Stakeholders	150
6.2.1.2	The consolidation of <i>Trust</i> values	151
6.2.1.3	Final CAESAR8 Checklist	152
6.2.1.4	Final rules and formula for the consolidation of CAESAR8 assessments	152
6.2.2	Web application	154
6.3	Implementing the final multi-stakeholder CAESAR8 model	158
6.3.1	Using CAESAR8 in Agile projects	159
6.3.2	Selecting Stakeholders	160
6.3.2.1	Consider Task for CAESAR8 Assessments	161
6.3.2.2	Choosing Stakeholders and not Influencers	162
6.3.3	CAESAR8 Implementation principles	166
6.3.4	Case Study - multi-stakeholder demonstration of the Gangs Matrix	167

6.3.4.1	Background	167
6.3.4.2	Methodology	168
6.3.4.3	Results	169
6.3.4.4	Discussion on the consolidation of <i>Trust</i> values	171
6.3.4.5	Conclusion	172
6.4	Earlier CAESAR8 prototype models	173
6.4.1	Development of first CAESAR8 prototype	173
6.4.2	Case Study - single assessment demonstration of the Gangs Matrix	173
6.4.2.1	Background	174
6.4.2.2	Methodology	174
6.4.2.3	Results	175
6.4.2.4	Conclusion	178
6.4.2.5	Known limitations to this early case study . .	179
6.4.3	Combining CAESAR8 assessments	179
6.4.4	Adding a tolerance value to the consolidation rules . .	180
6.4.5	The Excel Consolidator prototype	182
6.4.6	Case Study - The Boeing 737 MAX	185
6.4.6.1	Background	186
6.4.6.2	Methodology	188
6.4.6.3	Results	188
6.4.6.3.1	Individual assessments	188
6.4.6.3.2	Consolidator results	190
6.4.6.4	Conclusion	191
6.4.7	Removal of tolerance variable	192
6.4.8	Consistency of CAESAR8 Assessments - a synthetic case study	193
6.4.8.1	Purpose	193
6.4.8.2	Method	193
6.4.8.3	Results	194
6.4.8.4	Conclusion	195
6.5	Initial concepts for the CAESAR8 model	196
6.5.1	First concept of a circular model based on 6Ws	196

6.5.2	Second concept with separate strategic disciplines	197
6.5.3	Discontinuing with the 6Ws categorization	198
6.5.4	Designing the eight domains into the CAESAR8 model	203
6.6	Conclusion of Design and Development	205
7	Evaluation	206
7.1	Methodology	206
7.1.1	Two-part evaluation process	207
7.1.2	Ethical approval obtained	207
7.2	Procedure	207
7.2.1	Questionnaires (Pre and Post Eval)	208
7.2.2	Volunteer Training for the web app	209
7.3	Assessment criteria	209
7.3.1	Assessing the Problem Identification	210
7.3.2	Assessing the Design Goals	212
7.4	Participant characteristics	214
7.5	Results of Evaluation	217
7.5.1	The 15 problems areas	218
7.5.2	The diversity and inclusivity of CAESAR8 assessments	222
7.5.3	Underlying Issues	224
7.5.4	Analysis of the Design Goals	226
7.5.5	The efficiency of CAESAR8 assessments	234
7.5.6	Changes to the wording of performance markers fol- lowing the evaluation	237
7.5.7	Further analysis and discussion of results	240
7.5.7.1	Collective decision-making	240
7.5.7.2	Design style	242
7.6	Conclusion of Evaluation	243
8	Conclusion	245
8.1	A review of the five CAESAR8 design principles	247
8.1.1	Principle 1: Base artifact on a practical, holistic design	247
8.1.2	Principle 2: Gather multiple stakeholder perspectives .	247

8.1.3	Principle 3: Unify around a tractable checklist	248
8.1.4	Principle 4: Value process over EA artifacts	249
8.1.5	Principle 5: Provide a collective visualization	249
8.2	CAESAR8 in the context of EA theories	249
8.3	CAESAR8 and NIST organizational risk management	252
8.4	Limitations of CAESAR8	256
8.5	Further Development Opportunities	258
8.6	Future Research Opportunities	260
A	Node Analysis Table	286
B	Correlation values for sectors	289
C	Analysis of strong pairwise node correlation	291
D	Evaluation Questionnaires	307
D.1	Questionnaires	307
D.2	Response raw data	313
D.2.0.1	Key to response coding	313
D.2.1	Participant responses	314
D.2.1.1	Pre-evaluation 1 responses	314
D.2.1.2	Post-evaluation 1 responses	316
D.2.1.3	Pre-evaluation 2 responses	318
D.2.1.4	Post-evaluation 2 responses	319
E	Performance Marker Matrix - Question Set	322
F	Web app screenshots	327
G	Case study - synthetic scenario	334
H	Explaining the origins of the artifact to volunteers	338

List of Figures

1.1	Perspective of a potential A-EISA solution	7
1.2	Chapters and key sections of the thesis	15
2.1	Mind Map of all literature search areas	18
2.2	Search Keywords	20
2.3	Article publication dates	24
2.4	Code Distribution	28
2.5	Code Correlation with Success or Failure	28
2.6	Nodes positively correlated with a sector node	63
2.7	Different visualization formats	78
2.8	My interpretation of the PFIREES Four Phase model [139]	86
3.1	Using the DRSP model for the CAESAR8 artifact design	92
3.2	Evolution of CAESAR8 model over 5 iterations, resulting in the 5 CAESAR8 design principles for holistic ISRM and a CAESAR8 exemplar	94
3.3	Evaluation Strategy	98
3.4	Evaluation Strategy for CAESAR8	101
5.1	Pairwise correlation matrix for all 65 nodes	115
5.2	Node Scatter Diagram (success or failure versus pairwise cor- relation	116
5.3	Summary of the CAESAR8 domains and what they represent	119
5.4	Cobweb Diagram: shows strongest correlation between domains	120
5.5	Node scatter diagram showing coverage of the domains and the high-influence boundary	121

5.6	Nodes that have a strong influence value, or have a moderate or greater correlation to a strong influence node	132
5.7	Examples of the pairwise correlation analysis	133
5.8	High-influence and correlation for architecture-related nodes .	134
5.9	Count of the CAESAR8 levels identified in the pairwise analysis	137
5.10	Final CAESAR8 Matrix - version 2	139
5.11	Results presentation for CAESAR8	141
6.1	Main user input screens of the CAESAR8 web app	156
6.2	UML Class Diagram for the CAESAR8 web app	157
6.3	Javascript code to implement the consolidation formula	158
6.4	Using CAESAR8 in Agile projects	160
6.5	The example set of three organizational groups	164
6.6	Gangs Matrix Assessments - Case Study 3	170
6.7	The impact of different rules the consolidation of <i>Trust</i> values	171
6.8	CAESAR8 MS Excel Instantiation	174
6.9	Blank Excel CAESAR8 model with level 5 set as not applicable.	175
6.10	CAESAR8 Model Levels 1-4 Assessment for Gangs Matrix . .	176
6.11	MS Excel Consolidator <i>List</i> tab	183
6.12	Consolidation formula	183
6.13	Excel Consolidator at 50% tolerance value	184
6.14	Excel Consolidator at 20% tolerance value	185
6.15	CAESAR8 Group results for 737 MAX issues	189
6.16	CAESAR8 Consolidated results for 737 MAX issues	190
6.17	Case study results for researchers	195
6.18	First 6Ws cyclical design concept	196
6.19	Second 6Ws cyclical design concept, separating strategic disciplines	197
6.20	Summary of 6Ws category distribution	199
6.21	Distribution of the 15 problem areas under 6W's	201
6.22	Distribution of the 15 problem areas per domain	202
6.23	The 8 domain CAESAR8 model design	204

7.1	Average annual activity for professionals	216
7.2	Problems by category	219
7.3	Common problems matched to CAESAR8 benefits	219
7.4	CAESAR8 Benefits to address the 15 common problems	220
7.5	CAESAR8 Benefits to address the 5 stakeholder-related problems	220
7.6	Expert category split on 15 common problem areas as they were presented in the pre-evaluation questionnaire	223
7.7	Experts' views on the underlying (business) issues	225
7.8	Box-and-whisker for the experts' assessment of the 11 Design Goals	227
7.9	Answers that experts gave to the performance markers	232
7.10	Stakeholder involvement-related question responses	233
7.11	Box-and-whisker for user time-taken per performance marker in part 1 of the evaluation	235
7.12	Box-and-whisker for user time-taken per performance marker in part 2 of the evaluation	239
8.1	Multitiered organizational-wide risk management using CAESAR8 for a NIST Publication 800-39	254
8.2	Example metrics reporting based on Lean concepts	256
E.1	Performance Marker Matrix (or Question Set) v1	324
E.2	Performance Marker Matrix (or Question Set) v1c	325
E.3	Black and White performance marker matrix (or Question Set) v2	326
F.1	The web app Home Page	329
F.2	The Assessment page of the web app	330
F.3	The Results page of the web app	331
F.4	Training videos featured in the web app	332
F.5	Default options captured in the web app	333
G.1	Basic schema for the synthetic scenario	337

List of Tables

2	Abbreviations	xviii
4	Definitions	xix
2.1	Literature search and analysis	18
2.3	Systematic literature review search strings	22
2.4	Coding structure summary	25
2.5	A 6Ws EA matrix used by Zachman and SABSA	26
2.6	Correlation Coefficients	27
2.8	Nodes grouped by 6Ws categorization	31
2.9	Identification of IS problems in the literature review	32
2.10	Exploratory literature review topics	65
2.11	The 5 Levels	72
2.13	Search strings for finding similar artifacts	81
2.15	10 Theories for EA research	88
2.16	Literature review associated with design iterations	90
4.1	Lean and Agile design requirements	107
4.2	Additional design considerations	108
4.3	The essential design goals address the problems identified	112
5.1	Information Assets Domain	121
5.2	External Factors Domain	123
5.3	Technology Infrastructure Domain	124
5.4	Business Process Domain	125
5.5	Enterprise Architecture Domain	126
5.6	Security Governance Domain	127

5.7	Management Influence Domain	129
5.8	Human Factors Domain	129
5.9	The five CAESAR8 levels	136
5.10	Basic structure of CAESAR8 matrix	137
6.1	Overview of CAESAR8 model design, development and evaluation	145
6.2	Design iterations of the artifact and how they address the Design Goals	146
6.3	How CAESAR8 supports Agile values	159
6.4	Task Categorization	161
6.5	DPA contraventions mapped to CAESAR8	177
6.6	Problems distribution for the 6W questions	200
6.7	CAESAR8 domain problem distribution	201
7.1	Evaluating the problem areas between pre and post evaluation questionnaires	211
7.2	Evaluating the Design Goals	213
7.3	Evaluation volunteers for part 1 and part 2	215
7.4	Correlation between experts' findings for the fifteen problem areas	241
A.2	Node Analysis	288
B.2	Sector Node Correlations	290
C.2	Analysis of strongest pairwise nodes	306
D.1	Key to response coding	313
D.3	Pre-evaluation 1	315
D.5	Post-evaluation 1	318
D.7	Pre-evaluation 2	319
D.9	Post-evaluation 2	321
E.1	First version of the CAESAR8 performance marker matrix	323

F.1 CAESAR8 web app Screenshots 328

Abbreviations

The following abbreviations are used in the thesis:

Abbreviation	Meaning
6W	What, Who, When, Where, Why and hoW
A-EISA	Agile Enterprise Information Security Architecture
ACV	Artifact Concept Version
ACM	Association for Computing Machinery
ADM	Architecture Development Method, forms the core of TOGAF
APV	Artifact Prototype Version
BP	Business Process (sometimes abbreviated BP1, BP2,...,BP5)
CAESAR8	Continuous Agile Enterprise Security Architecture Review in 8 domains
CISO	Chief Information Security Officer
CMM	Capability Maturity Model
CSS3	Cascading Style Sheets version 3
DMAIC	Define-Measure-Analyze-Improve-Control
DPO	Data Protection Officer
DSR	Design Science Research
DSRP	Design Science Research Process
DMU	DeMontfort University
EA	Enterprise Architecture (sometimes abbreviated EF1, EF2,...,EF5)
EF	External Factors (sometimes abbreviated EF1, EF2,...,EF5)
EISA	Enterprise Information Security Architecture
ESA	Enterprise Security Architecture (same as EISA)
FAA	Federal Aviation Administration
GDPR	General Data Protection Regulation
HF	Human Factors (sometimes abbreviated HF1, HF2,...,HF5)
HTML5	HyperText Markup Language version 5
IA	Information Assets (sometimes abbreviated IA1, IA2,...,IA5)
ICO	Information Commissioner's Office
IDE	Integrated Development Environment

IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IS	Information Security/Systems
ISM	Information Security Management
ISRM	Information Security Risk Management
IT	Information Technology
KPI	Key Performance Indicator
MCAS	Boeing Maneuvering Characteristics Augmentation System
MI	Management Influence (sometimes abbreviated MI1, MI2,..MI5)
MPS	Metropolitan Police Service
N/A	Not Applicable
NIST	National Institute of Standards and Technology
OT	Operational Technology
PDCA	Plan-Do-Check-Act
RAG	Red, Amber, Green
RBAC	Role-based Access Control
Rel	Relevance (score)
RM	Risk Management
RQ	Research Question
SABSA	Sherwood Applied Business Security Architecture
SG	Security Governance (sometimes abbreviated SG1, SG2,....,SG5)
SME	Small to Medium-sized Enterprise or Subject Matter Expert
SVG	Scalable Vector Graphics
TI	Technology Infrastructure (sometimes abbreviated TI1, TI2,....,TI5)
TOGAF	The Open Group Architecture Framework
TUPE	Transfer of Undertakings (Protection of Employment)
TPS	Toyota Production System
UK	United Kingdom
VBA	Visual Basic for Applications

Table 2: Abbreviations

Definitions

The following definitions apply in the thesis:

Term	Meaning
Administrators	Personnel who administer the artifact
Aggregating Assessments	Consolidating Assessments
Artifact	The CAESAR8 Model
EA Artifact	Architecture Documentation
Eval	Evaluation
Expert	Volunteer in the artifact evaluation
Participant	Volunteer in the artifact evaluation
Respondent	Person responding to evaluation questionnaire
Stakeholder	Person who is affected by a business project
Tool	The CAESAR8 Model
The University	De Montfort University
Users	Users of the model, e.g., stakeholder or SME
Volunteer	Expert taking part in the artifact evaluation

Table 4: Definitions

Chapter 1

Introduction

An enterprise can be regarded as a complex system that is made up of multiple domains that all have an influence on each other [78]. These domains include people, data, processes and technology. Enterprise Architectures (EAs) describe how these domains relate to each other with the aim of providing an explicit description of these relationships. These explicit descriptions are defined in EA artifacts, which collectively form the EA documentation.

An EA framework that is specifically designed for information security risk management (ISRM) is commonly referred to as an Enterprise Information Security Architecture (EISA).

1.1 The theoretical benefits of EA/EISA

Organizations that follow an EA approach when designing new information systems are then able to obtain an accurate understanding of the true effects that a change will have on the business strategy and its operations [164, 106, 5]. EA artifacts document how the business operates and describe how business assets and processes are dependent on information technology services.

Adopting the practice of EA in the design and implementation of security strategies will help companies manage complex business processes and support business strategies [63, 179]. In addition to ensuring that routine tasks

operate reliably and predictably [44, 63, 81], it can also facilitate double-loop organizational learning [175], where strategies are monitored for their effect and improved if necessary. This process can even help management to seek out business change opportunities [170]. Without this level of organizational structure, knowledge of the business could become isolated into silos, with executives initiating business change with a limited perspective on the wider implications for its information security.

Therefore, information security benefits from this architectural approach, because it encourages the integration of security in all aspects of the design of information systems [109]. Adopting an EISA approach for ISRM provides a security strategy that is focused on business requirements [106, 5]. But much like the conventional architecture of buildings, it also needs to consider the goals, the environment, and the resources available to build and maintain it [154]. Failure to integrate security requirements throughout the design of information systems can result in security being treated as an add-on, potentially increasing costs, causing delays and limiting its effectiveness [38].

The pursuit of innovation and efficiency in modern organizations is undertaken in an environment of increasing complexity, coupled with unprecedented increases in data volumes. Indiscriminately following generic security standards or applying outdated frameworks may not match the risk profiles of organizations, and may not provide adequate protection of information [167, 179]. Senior executives are often aware of the need to embrace these new technologies but are not always considering the security risks that these technologies can incur for their business, as security is often traded for usability without due diligence being applied.

For example, some of the latest advances in technology, such as the Internet of Things (IoT), require that organizations take an holistic view (which EA provides) as to how they secure information and services, since some new technologies may have least-complexity and are unlikely to be innately secure [1].

Another example of new technology is cloud-computing. Where an organization's data becomes distributed and decentralized, such as in the case of cloud-based services and artificial intelligence (AI) initiatives, consideration

should also be given to the security arrangements of these services and of their partners that are providing the services [66, 166, 73]. The risks from new technology and business change can grow unchecked [112] if an organization focuses its information security strategies solely on its traditional systems [2, 54, 31, 171, 92]. Due to these rapid advances in technology, organizations should look beyond traditional corporate network boundaries when looking at how to protect their data, to ensure that their information security strategies are effective [166].

The needs for information security are pervasive throughout the enterprise architecture. Therefore, both business architecture and IT architecture need to be considered holistically in order to select the most appropriate security models [67]. Security should not unduly hinder business function, but business processes should have due regard to security constraints, including legislative and regulatory requirements [9, 105, 126].

1.2 The practical problems for EA/EISA

In reality, there are barriers to achieving the benefits of EA in general [110] and these are also applicable to EISAs. For example, even where an EA has been implemented within an organization, it may be incomplete (e.g. partially implemented for a certain project only) or unreliable (e.g. not being maintained or difficult to interpret). This can result from the fact that EA documentation is often implemented to support technical projects [15, 22]. Focusing only on delivery of the technical architecture ignores the other interrelated domains. This approach can fail to address the wider business context because technology is only one component in the overall company strategy [154] and therefore any impact assessment based on these EAs could be inaccurate.

Most EA frameworks do not include all of the essential information security details [117]. In worst cases, security risk management can be left to developers working on IT assets [53], who then decide what security controls to implement. Many of the risk models in use lack the ability to model tech-

nology risk from an enterprise activities perspective [11].

These issues can also result in organizations departing from their established architectures in order to deliver solutions faster, thereby losing the benefit and compromising their architecture in the process [150].

Business strategies need to quickly adapt to market trends, therefore, information security strategies should change to ensure continual alignment [163].

Another problem for EAs is the capturing of tacit knowledge held within the business when making judgments on enterprise information security risks [98]. Much of this tacit knowledge cannot be committed to EA artifacts, so EA documentation cannot provide the explicit knowledge required. When making information security decisions without this tacit knowledge, much has been studied about cognitive illusions and uncertainty when attempting to make accurate judgments [129]. For information security, the resulting subjective confidence can hide errors in information security judgments. The dynamic involvement of stakeholders across the domains affected by a change will be required to capture this tacit knowledge.

Examining commercial tools for risk assessing information security shows that these are often based on matrices that involve subjective mathematical assessments and lack the holistic perspective that EA provides. Such methods are prone to the problems of subjectivity when trying to quantify risks where the severity and likelihood are negatively correlated [6]. Cox describes how categorizing the severity of risk reflects the assessor's personal experience. This form of quantitative risk rating requires judgments to be made by individuals and "the potential for inconsistencies in how they are made by different people, implies that there may be no objectively correct way to fill out a risk matrix".

There is appreciation of the theoretical benefits of EA in the science literature but the lack of practical research in this field prevents many organizations from overcoming the problems described above and allowing organizations to achieve the theoretical benefits of EA. These problems are increasing, for example, due to the complexities of cloud computing and rapidly evolving digitization strategies. Therefore, many aspects and characteristics of how

the enterprise conducts its business remain tacit.

Modern businesses need to change and adapt very quickly to remain competitive but there has been very little research in relation to how EA can be aligned to changes in business [88]. Korhonen et al. [96] offered one perspective that called for a “radical re-conceptualization to inform a more adaptive EA practice”. This suggested a need for EA to be more coherent with a continuous evolution with the business environment, where EA is a shared competency and everyone becomes involved with EA. This approach is very much aligned with my artifact’s contribution, as the CAESAR8 model blends the knowledge of multiple business stakeholders who conduct continuous, independent assessments.

There are many commercial EA and EISA frameworks, including Zachman [184], TOGAF [64] and SABSA [154], but these have many implementation issues, such as their stipulation on creating specific documentation and their step-wise methodologies for integrating EA activities with the business [99]. The effort in achieving and maintaining these architectures, such as the problems in agreeing and maintaining EA artifacts, can be difficult for management to accept. Constructing and maintaining a complete EA from scratch can be very difficult, because it requires substantial resource and commitment [89], hence the majority of EA practical implementations do not resemble the theoretical EA frameworks [98].

Many commercial frameworks advocate a centralized approach for implementing EAs. For example, TOGAF [64] version 9.1, page 17, states: “an enterprise architecture practice must be run like any other operational unit within a business, i.e., it should be treated like a business”. Whilst this may be good for an EA function, it would be too costly for smaller enterprises.

Most academic research has tended to focus on EA from its understanding and modeling, rather than EA management in practice [57]. However, Ross et al. [141] recommend adopting EA as a compass and using individual projects to *build out* the architecture by ensuring that individual stakeholders share the goals and risks to achieve company-wide synergies.

In summary, my study determined that: EAs are valuable for assessing the risks of information security; but commercial frameworks are largely theoretical and have problems in their implementation. Therefore organizations need practical solutions that will help them overcome the barriers to adopting an EA-based approach.

1.3 Motivation behind my research

As an experienced information security professional with 37 years experience, I have been aware of the potential value of EAs for improving the accuracy of information security risk assessments.

For many years I have pursued the EA discipline but have struggled to gain organizational-wide acceptance for fully implementing any of the popular frameworks within small to medium-sized (SME) organizations. I have successfully used elements of EA and have received positive recognition for my pursuit of EA, but I have frequently failed to get EA accepted as a concept that the c-suite was willing to commit to on a *business-as-usual* basis. I understand some of the reasons for this rejection and had a number of misgivings for the various popular frameworks available. For example, the requirements for implementing some of the components of a framework can be unclear. Also, producing EA artifacts that other teams will accept and follow is not an easy task. Significantly, the EA approach and the creation of EA documentation does not support an important agile principle (“Responding to change over following a plan” [17]) when meeting the constant flow of business change. A new approach was urgently required to assist organizations to use EA, especially for SMEs.

Figure 1.1 captures some of the empirical evidence of the challenges for EA that I held before I started my research. For example, I had witnessed how the type of organization can affect executive decisions over long-term investments. In organizations with vertical command structures, senior executives may seek quick results in preference to long-term investments for

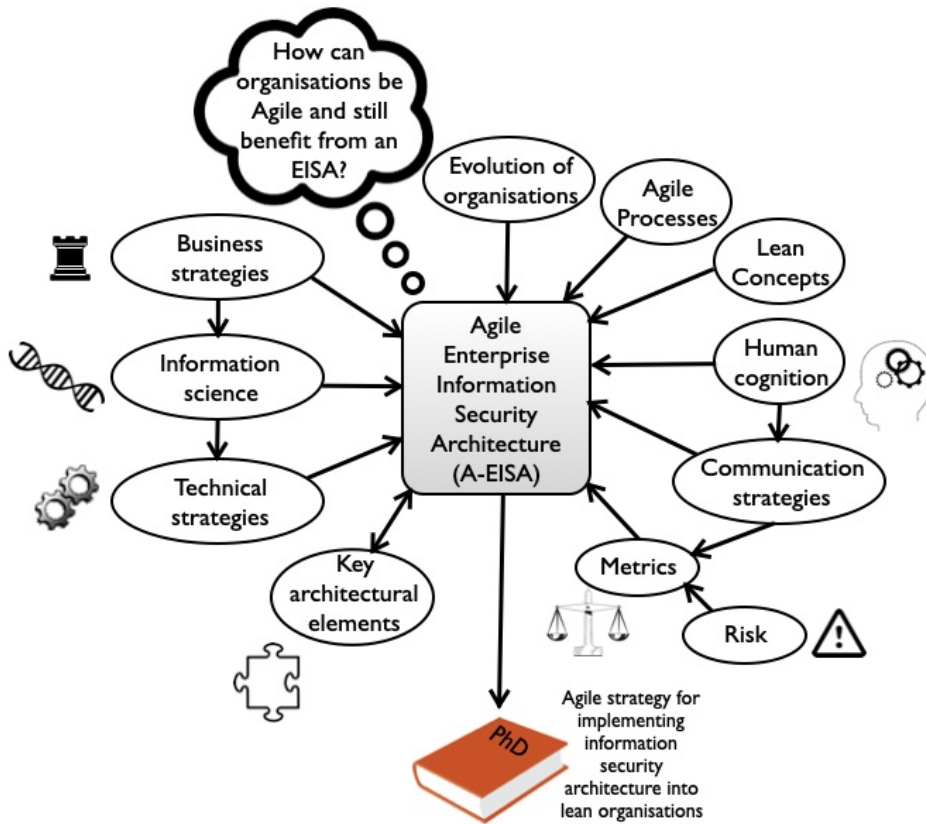


Figure 1.1: Perspective of a potential A-EISA solution

IT/IS. Also, the way that information security risks are communicated to senior executives, and the metrics used, affects their interpretation and ultimately their response.

Aligning business and technical strategies is an important function of EAs but, in my experience, there is a tendency to jump too quickly to the technical elements of EA frameworks and skip the all-important *information* strategies that sit between the business and its technology. Also, understanding how human cognition impacts ISRM would be significant to understanding how to make EAs more effective.

EA approaches can also be contrary to the aims of a lean business; in other words, EA approaches are unlikely to be a suitable approach for organizations that are seeking to adopt a lean or agile approach to supporting their business. These two concepts can be seen as diametrically opposed.

I wanted to make sure that my research covered all of these areas, but first I needed to explore why organizations have been unable to adopt EA approaches to ISRM. Then, I would gain a better understanding of how organizations might be helped to benefit from an agile EA approach to ISRM.

1.4 Research aim

My study started with the following research question:

Agile Enterprise Security Architecture (A-ESA): how can traditional ESAs be optimized to serve the emerging behaviors of the lean enterprise?

The original aim of my research was to identify a way to help organizations implement existing commercial EA/EISA frameworks in agile environments. My study quickly identified that there was little scientific evidence that some of the commercial frameworks could deliver the expected benefits - or if they could even be implemented consistently.

A new approach was required that provides an holistic perspective when reviewing the information security risks for the ever-changing requirements of information security strategies [88].

The aim of my study, therefore, was to design a new artifact. Following Design Science methodology, my thesis describes the design and development of a novel model called CAESAR8 - Continuous Agile Enterprise Security Architecture Review in 8 domains. CAESAR8 provides a practical Agile approach to Enterprise Information Security Architecture (A-EISA) but CAESAR8 is not a new EA or EISA framework. CAESAR8 will support the implementation of any framework that might have been selected by an organization, but it only checks that projects are working on EA artifacts that are actually relevant to the current business changes. The CAESAR8 model can also be used standalone to provide a rapid and holistic review of the status of ISRM in any business change project.

1.5 Research questions

I devised two main research questions to address the aim of my study. For my first question I wanted to go back to first principles and study why ISRM still fails for many organizations, rather than base my research on the assumption that EA approaches are the solution for ISRM. My first research question was:

Research Question 1 (RQ1): Why do organizations fail to identify some key information security risks until incidents occur (the **Problems**)?

To answer this question and test my hypothesis that EA is theoretically beneficial to ISRM but difficult to achieve in practice, my first research question incorporated *intelligence-gathering* in the form of sub-questions for organizing my literature search:

Sub Question 1a (RQ1a): How do the root causes of information security incidents reflect failings in how an enterprise has conducted risk assessments for its information security programs (**IS Failures**)?

The first sub-question (RQ1(a)) was intended to examine security incidents to determine the enterprise-wide issues that are behind the failures of information security. I referred to this part of the search as *untargeted*.

Sub Question 1b (RQ1b): To what extent has EA already been seen as a potential solution to make information security risk assessments more effective (**EA Role**)?

The second sub-question (RQ1(b)) included explicit references to EAs, and I referred to this part of the search as *targeted*. It was intended to find literature that describes the impact of EA approaches in relation to IS performance. Separating RQ1a and RQ1b ensured that my research was not limited to the current use of EA frameworks.

Sub Question 1c (RQ1c): Are there any fundamental differences between the public and private sectors that need to be taken into consideration when taking an EA approach to information security (**Sectors**)? The third sub-question (RQ1(c)) was addressed by codifying any industry sector differences discovered in the literature.

The information obtained from all three the sub-questions allowed me to conduct root cause analysis into ISM failures. To ensure that my artifact incorporated just the most influential EA aspects for ISRM, I used the results of this analysis when addressing my second research question to find a solution. My second research question was:

Research Question 2 (RQ2): How can organizations adopt a more agile approach to using EA in information security risk assessments (the **Solution**)?

(The bold text included in parentheses are abbreviations to the research questions in the thesis.)

1.6 Research contribution

In meeting my research aim, I have made substantive contributions to the body of knowledge. My research has identified five novel design principles that should be observed when creating a model that will provide an holistic but agile solution for the continuous assessment of information security risks during business change projects. The five design principles are:

Principle 1: Base artifact on a practical, holistic design. An Enterprise Architecture (EA) provides theoretical benefits for Information Security Risk Management (ISRM). However, many commercial EA frameworks do not deliver these theoretical benefits. Therefore, research into EAs for the purpose of ISRM should not be based solely on commercial frameworks that have little or no proven benefit.

Principle 2: Gather multiple stakeholder perspectives. All business stakeholders that are affected by a business change should be included in an ISRM process to obtain their applicable tacit knowledge. Stakeholders should be allowed to offer their knowledge in a way that is free from the dangers of groupthink.

Principle 3: Unify around a tractable checklist. An ordered and tractable checklist should be used when conducting ISRM for agile business change projects. The checklist should examine a common set of enterprise problems that are at the root cause of IS failures, and allow affected business stakeholders to repeatedly check that these problems are being avoided.

Principle 4: Value process over EA artifacts. The holistic process for ISRM is more important than creating EA artifacts. EA artifacts can be difficult to create, difficult to use and a problem to maintain. This causes delays and expense. In other words, the journey can be more important than the destination.

Principle 5: Provide a collective visualization. The results of ISRM need to be shared by all those affected by a business change and in a format that supports senior management engagement and intervention.

As a result of completing five design and development iterations, I have created and then evaluated a nascent *abstract exemplar* model that is based on these five design principles, which I have called CAESAR8. I provide this CAESAR8 model as an example of how the five design principles can be implemented as a practical solution to the business community.

1.6.1 Designing a practical solution that suits agile projects

CAESAR8 is a process-centered EA model, but it is one that follows the business process, not a specific EA process. The creation of EA artifacts is

incorporated but not a mandatory requirement. Therefore, this model enables organizations to obtain the benefits of an EA-approach for dynamically assessing information security risks, but without the problems commonly experienced by architects following a commercial EA framework, such as the costs and obstacles associated with implementing and maintaining EA documentation.

The model is designed to support information security strategies, so it is specifically focused on EISAs. As with all EAs, when an EISA is implemented successfully, it uncovers otherwise hidden risks and helps to determine how adjustments should be made to security and safety strategies in real-time, thus enabling business change and innovation [63].

CEASAR8 captures and combines the tacit knowledge held in organizations, and incorporates an holistic checklist of critical success factors that will guide multiple stakeholders in providing a continuous review across of information security risks. To support an agile approach, the model focuses reviews on the most critical factors that help ensure business change projects are successful [109]. This review considers eight specific domains: Enterprise Architecture, External Factors, Security Governance, Business Process, Information Assets, Technology Infrastructure, Human Factors and Management Influence. The results are visualized across these eight domains and provide instantly share-able information security metrics on the progress of a business change project. This ensures that common problems areas for information security risks are being fully considered by a project.

CAESAR8 supports an organization's rapid response to change, as the agile concept is an intrinsic characteristic, and helps to protect the security culture within the organization. However, CAESAR8 is not aligned to any specific agile project methodology. CAESAR8 will allow organizations to integrate the model into any agile project, ensuring that security risks are assessed both holistically and iteratively, and it fully supports the four agile values that are described in the agile manifesto [17] *i.e. individuals and interactions over processes and tools; working software over comprehensive documentation; customer collaboration over contract negotiation; and,*

responding to change over following a plan. On the basis of my findings, adherence to these overarching agile *values*, and maintaining an agile mindset throughout a project is more significant for *agility* than aligning to a specific agile methodology [56].

1.6.2 Designing a practical solution that suits the smaller business

The author's experience of assessing information security risks within many and varied organizations over several decades has demonstrated how thinly implemented the concepts of EA are within business, particularly for smaller organizations. Existing architecture frameworks typically require extensive knowledge of other standards and concepts, with skill and time required to selectively incorporate them into the architecture [89].

Even when organizations have implemented parts of an EA, they tend to make compromise decisions and depart from the architecture in fundamental ways to deliver IT solutions faster, but, in the process, rendering the architecture ineffective [150].

I possessed empirical knowledge of the challenges faced by SMEs when trying to adopt EA approaches for information security risk decisions and I made a very conscious decision not to conduct more research on the theoretical concepts of EA. Instead, I chose to focus my research on the design of a new model that would provide organizations with a practical solution for following an EA approach for information security risk assessments.

CAESAR8 has been designed to allow organizations to immediately benefit from an holistic approach when assessing information security risks but does so without the need for organizations to incur the traditional overheads, such as the cost of expertise or the time to create EA artifacts, which are commonly experienced with an EA approach [89].

For smaller organizations, where information security can often be regarded less of an enterprise issue and more of a technical problem [29, 52], the model can be used as a standalone tool to ensure that information security is considered more holistically right from the start of the project and continuously

thereafter as the project matures.

1.6.3 A shared architecture concept

To ensure that reviews are truly holistic and encompass all relevant knowledge about the business, the model obtains the independent reviews of all key stakeholders affected by a business change project. These differences in stakeholder knowledge and experience are assessed separately and then consolidated into a single assessment result.

The questions to stakeholders in the CAESAR8 checklist are called *performance markers*. They represent key information security knowledge and require no expert security knowledge from the stakeholder. It is only essential that stakeholders completing the checklist have full knowledge of the status of these performance markers in the context of their own business area. Similarly, the CAESAR8 result requires no specialized interpretation and can be shared at all levels of the organization.

Incorporation of human behavioral-science¹ into the design of CAESAR8 is a major contribution of my research. Bringing together the perspectives of diverse stakeholders reduces the over-dependency on individual experts and increases the accuracy of the overall assessment [129]. It also helps to alleviate another challenge for many organizations, where their business operations tend to operate in silos [46].

In effect, CAESAR8's design enables all stakeholders to become architects, which encourages their commitment and participation.

1.7 Structure of thesis

Figure 1.2 shows the chapters of the thesis and the main sections that these contain. The key associations between the chapters are also shown.

¹The application of scientific principles to the study of the behavior of organisms [35].

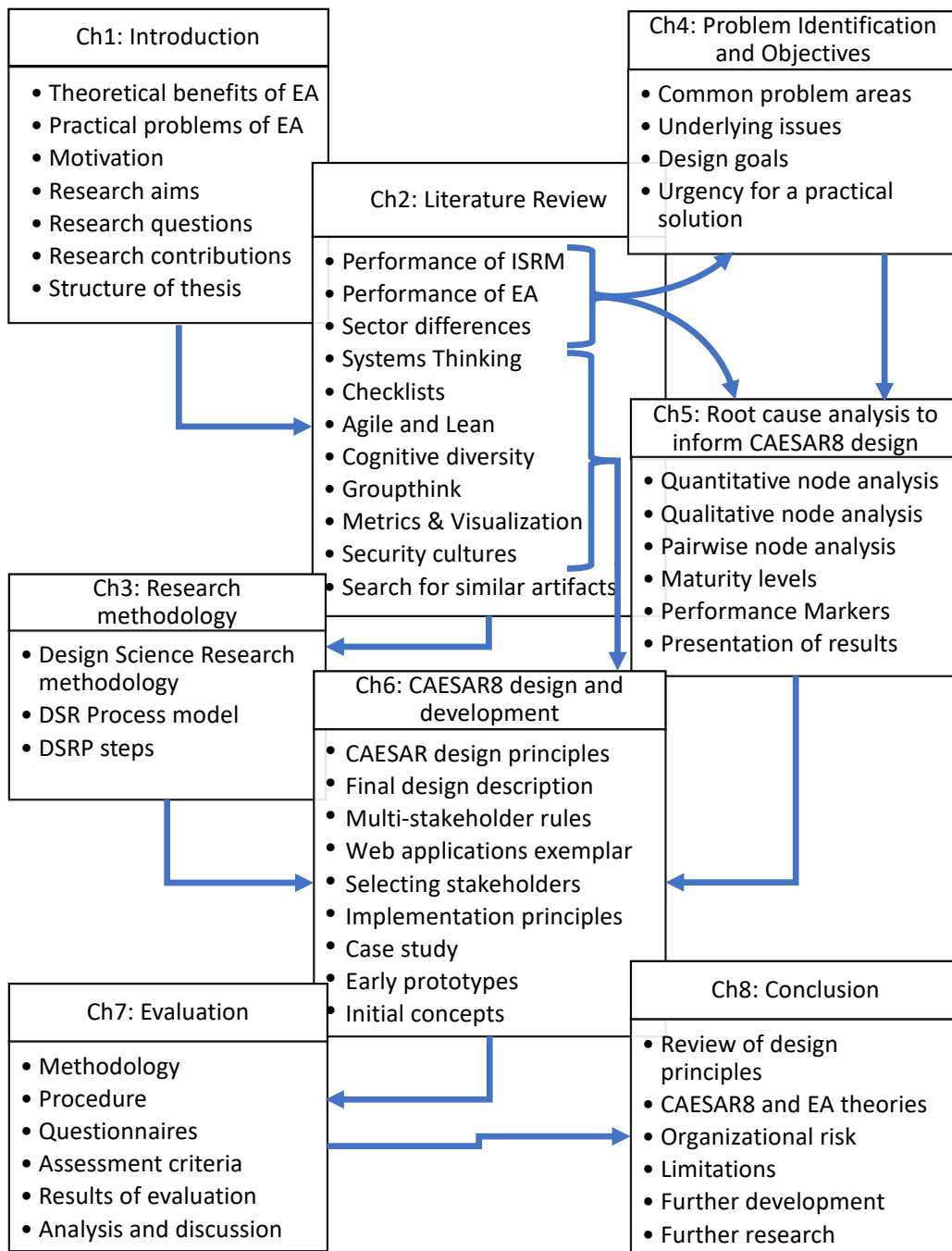


Figure 1.2: Chapters and key sections of the thesis

1.8 Conclusion of Introduction

In this chapter, I have described the theoretical benefits of EA/EISA approaches for increasing the reliability of ISRM. However, I have then discussed the problems that exist in achieving those benefits in practice when using existing commercial frameworks. Having gained empirical evidence of these problems from my experience in the industry, I explained how these challenges are compounded for small to medium enterprises (SME) with limited resource and also those organizations that are trying to embrace Agile values and Lean principles for business change projects.

I created research questions with the aim of uncovering the key problems for ISRM using a first-principles approach and I explained how I have used this approach to gather intelligence for designing a practical solution for SMEs. My research has identified five novel design principles that are required for a practical solution to ISRM that is both agile and holistic. I summarize these design principles as the CAESAR8 model and they form my substantive research contribution to the body of knowledge.

I have developed an exemplar CAESAR8 web application based on these design principles and I used this instantiation of the CAESAR8 model to conduct a rigorous evaluation of the results of my research with industry experts.

I close the chapter by providing a map to my complete dissertation on the CAESAR8 model, its chapters and main sections.

Chapter 2

Literature Review

To address my research questions, my literature review was conducted in two phases. The first phase was a systematic literature review to find all relevant academic literature for my first research question (RQ1) and its sub-questions - identifying the problems for A-EISA. The second phase involved multiple explorations of the literature to address relevant areas of my second research question (RQ2) - finding the solution for A-EISA.

2.1 Search plan

My literature search for developing a practical A-EISA solution for SME organizations was multifaceted. To help answer my research questions, I conducted multiple searches (both systematic and exploratory) and then conduct further analysis of the literature.

I structured my search as shown in Figure 2.1, which is a mind map that has the A-EISA domain as its central theme. The search topics were partly influenced by my empirical knowledge of the domain as an experienced information security professional, but they also developed as the artifact matured through demonstrations of its design and development iterations.

The systematic literature review for research questions RQ1a to RQ1c are shown as *green* boxes in Figure 2.1; and the topics for the exploratory

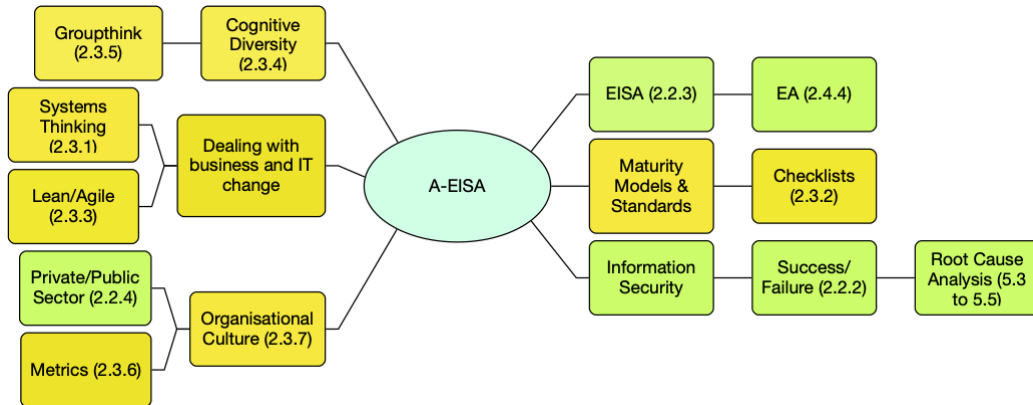


Figure 2.1: Mind Map of all literature search areas

searches of the literature to answer research question two (RQ2) are shown in the *yellow* boxes.

Table 2.1 provides a summary of how the literature search and analysis was organized around my research questions. The numbers in brackets identify the sections where this study is described in the thesis, and the bold text are abbreviations to my research questions, as defined in Section 1.5.

RQ1a	RQ1b	RQ1c	RQ2
IS Failures	EA Role	Sectors	Agile Solution
Systematic literature review (Sec.2.2)			Exploratory literature review (Sec.2.3)
Problem identification (RQ1) (Sec.4.1.1)			Root cause analysis of systematic literature review (Ch.5)
Objectives of the artifact (Sec.4.2)			

Table 2.1: Literature search and analysis

2.2 Performance of information security risk management

This systematic literature review was designed to gather key intelligence for my research, as described in Section 1.5, and provided answers to my three sub-questions for RQ1.

2.2.1 Applying the Systematic Literature Review methodology

This literature review followed a systematic approach in order to find all information applicable to my research [90, 68, 165]. My review was structured as follows:

1. Defining the search plan;
2. Specifying inclusion and exclusion criteria;
3. Selecting keywords for the search;
4. Creating Boolean search strings;
5. Selecting the analysis method(s);
6. Selecting the literature; and,
7. Analyzing and synthesizing the data.

Initial selection was based on a review of document title and abstract. Articles that were older than two years and had no citations were still considered, but with a view to rejecting them. Selected articles were saved in Zotero, where they were examined in more detail and some papers were rejected. The resulting articles were then transferred to QSR NVivo for detailed analysis. This would provide statistical data for the quantitative analysis phase.

2.2.1.1 Inclusion criteria

My artifact is aimed at providing enterprise-level reviews of information security risks, so my search criteria were designed to identify academic studies of information security incidents, as opposed to capturing the detailed technical study of specific attacks.

As a commercial concept, EISA started to gain recognition circa 2005 [23, 152], and the Agile approach was being developed in the 1980's and 1990's.

Therefore, I restricted the search to ten years, from 2005 to 2016 (the search was undertaken at the beginning of 2016).

Only academic research papers were included in the review, and all literature was sourced from the databases: IEEE Xplore, ACM and SCOPUS. IEEE and ACM databases were chosen as they provide comprehensive sources for researching cybersecurity, and SCOPUS is the largest multidisciplinary, peer-reviewed database.

2.2.1.2 Exclusion criteria

I excluded articles that are not written in the English language, articles older than two years with zero citations, and non-academic papers.

2.2.1.3 Search keywords

Figure 2.2 shows my search keywords. As mentioned in Section 1.5, I created two separate collections, *non-targeted* (i.e. root causes, top half of Figure 2.2) and *targeted* (i.e., architecture implementations, bottom half of Figure 2.2). Searches were restricted to article meta data and abstract only. All papers were selected and analyzed by myself, as an experienced information security professional.

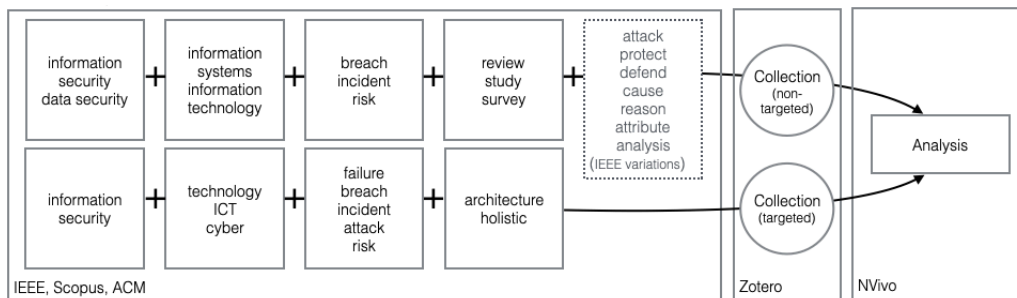


Figure 2.2: Search Keywords

The use of keyword variations for IEEE (shown in the dotted box) was used to narrow the search results for this database. An explanation of this search is provided in the next section.

2.2.1.4 Search strings

Table 2.3 shows the boolean search strings that were used in the search for literature.

Database IEEE non-targeted standard search was returning 1000 hits. For this reason, I varied the search string keywords for the IEEE non-targeted, to narrow the search and identify the most suitable articles for my literature review and analysis. The keyword variations are shown in Figure 2.2 and the three separate IEEE search strings for non-targeted are identifiable in Table 2.3.

RQ#	Db	Boolean expressions used	Result	Select	Total
RQ1a (non-targeted)	IEEE	(“information security” OR “data security”) AND (“information systems” OR “information technology”) AND (breach OR incident OR attack OR protect* OR defen*) AND (cause OR reason OR attribut*) AND (analys* OR review OR study)	185	23	41
(+)		((“information security” OR “data security”) AND (“information systems” OR “information technology”) AND (breach OR incident) AND (protect* OR defen* OR “lower risk”) AND (analys* OR review OR study))	45		
(+)		((((“information security” OR “data security”) AND (“information systems” OR “information technology”) AND (“data breach” OR “security breach” OR incident OR “information risk”) AND (review OR study OR survey))))	59		

RQ#	Db	Boolean expressions used	Result	Select	Total
RQ1a (non-targeted)	SCOPUS	ABS(("information security" OR "data security") AND ("information systems" OR "information technology") AND ("data breach" OR "security breach" OR incident OR "information risk") AND (review OR study OR survey)) AND PUBYEAR > 2005 AND DOCTYPE (ar)	24	15	
RQ1a (non-targeted)	ACM	(+"data security" + "information security" + "information systems" "information technology" "data breach" "security breach" incident "information risk" review study survey)	10	3	
RQ1a (targeted)	IEEE	("information security" AND (architecture OR holistic) AND (technology OR ict OR cyber*) AND (failure OR breach OR incident OR attack OR risk))	287	31	43
RQ1a (targeted)	SCOPUS	ABS ("information security" AND (architecture OR holistic) AND (technology OR ict OR cyber*) AND (failure OR breach OR incident OR attack OR risk)) AND PUBYEAR > 2005 AND DOCTYPE (ar)	24	7	
RQ1a (targeted)	ACM	("information security" AND (architecture OR holistic) AND (technology OR ict OR cyber*) AND (failure OR breach OR incident OR attack OR risk))	37	5	

Table 2.3: Systematic literature review search strings

2.2.1.5 Search results

After de-duplication and removal of irrelevant articles, 41 documents were selected for B1 non-targeted search collection. During pre-analysis further article(s) were removed from the analysis:

- 1 article was removed, as the body of the document was not in English language.
- 1 article was removed, as only obtained abstract information.
- 1 article was removed, as a subjective analysis of perceptions contained in extant literature.
- 2 articles were removed, as too technology-specific.
- 1 article was moved to *security standards* analysis.
- 7 articles were moved to *risk management* analysis.

Final non-targeted (general incident) collection total for detailed analysis was **28 articles**.

After de-duplication and removal of irrelevant articles, 43 documents had been selected for RQ1 targeted search collection. During pre-analysis further article(s) were removed from the analysis:

- 6 articles were moved to *ESA* analysis, as they specifically related to enterprise architecture and were not relevant for RQ1a analysis.
- 1 article was moved to *risk management* analysis.
- 2 articles were removed as being non-academic and too technology-specific.

Final targeted (those with architectural references) collection total for detailed analysis was **34 articles**.

Therefore, a total of 62 articles were used for the detailed analysis, and the publication date for these articles is shown in Figure 2.3. I concluded from the graph that there was no discernible increase over time for architecture

references in the context of information security incidents. Further analysis actually showed a small decline in architecture references, but this amounted to less than one article over the 10 year period.

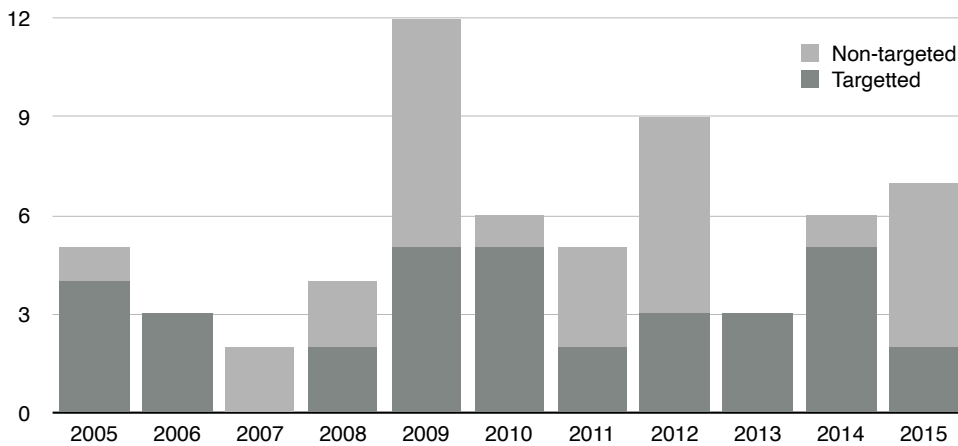


Figure 2.3: Article publication dates

2.2.1.6 Analysis method

My search for literature had identified 62 articles that were suitable for detailed analysis. This analysis of the literature was conducted in 3 phases:

1. All 62 articles were read in full and coded in QSR NVivo. Figure 2.4 shows the total number of references for each node¹.
2. A review of the specific NVivo node references was made to observe key issues that govern success or failure. The main points were noted in the context of the 6Ws². This work is described in Section 2.2.2.
3. Root cause analysis was later conducted on the coding in the literature to determine what the key factors are for successful information security strategies.

¹A *node* is a container in NVivo coding. I created Nodes at the points in articles where relevant topics for my research are located. Sometimes, several nodes intersect at these points in an article, for example: *information sharing*, *public sector* and *failure* nodes.

²The 6Ws is a recognized set of questions (interrogatives) used for information gathering and problem solving. They are: *Why, When, Who, What, Where and How*

I created NVivo nodes dynamically as the articles were read in full. The node names and structure were specifically not predetermined. A study has shown that understanding is not synonymous with prediction - experts in a particular field are much better at selecting and coding information than they are at integrating it [42]. Dynamically creating the nodes ensured that the root causes of security failures and successes were captured with an appropriate level of granularity. Nodes were created on the basis of evidence of failures or successes; for example, where the literature identified the node as being the cause of failure or referred to the node as being a benefit to ISRM. I did not include future predictions.

In total, I created 65 nodes that capture the potential root causes of success or failure of information security. In addition to nodes for root causes, I created additional nodes to indicate whether the reference described a cause of failure or success, and this gave me the information that I required to answer research questions RQ1a and RQ1b.

In order to answer research question RQ1c, I also included a node for public or private sector, where an article made a clear distinction.

A summary of my coding structure to support the analysis for answering RQ1 is provided in Table 2.4.

Root cause	Effect	Sector
RQ1a, RQ1b	RQ1a, RQ1b	RQ1c
65 nodes	Failure/Success	Public/Private

Table 2.4: Coding structure summary

6Ws categorization. To provide structure for the analysis, I studied the findings of the systematic literature review using the 6Ws categorization.

This form of interrogation has long been formalized in the fields of education, journalism and science, and these are already used in some EA/EISA frameworks, such as the Zachman [184] (EA) and SABSA [154] (EISA). In these frameworks, the 6Ws interrogatives typically form the columns of the model, and the rows provide different perspectives of the architecture, forming a two-dimensional matrix. For example, see Table 2.5.

	Why	When	Who	What	Where	How
Scope/ Contextual						
Business/ Conceptual						
System/ Logical	Cells provide the ontology for describing the enterprise					
Tech./ Physical						
Detail/ Component						
	Motivation	Time	People	Assets/ Data	Location/ Network	Process/ Function

Table 2.5: A 6Ws EA matrix used by Zachman and SABSA

Following inspection of the code references in NVivo, the Nodes were then categorized into the most appropriate W categories so that common issues could be reviewed together.

Note on correlation values. In my analysis of the literature coding, I often refer to correlation values. I examined the correlation between success or failure nodes, business sector-specific nodes and between individual nodes, e.g., for my pairwise analysis of the most influential nodes.

For these calculations, I have used the Pearson’s r correlation coefficient ($-1 \leq r \leq +1$), and it defines the linear correlation between two nodes in my coding. Asuero et al. [7] provide a rule-of-thumb scale for evaluating correlation coefficients and I have reproduced this in Table 2.6.

Size of correlation	Interpretation
0.90 to 1.00	Very high correlation
0.70 to 0.89	High correlation
0.50 to 0.69	Moderate correlation
0.30 to 0.49	Low correlation
0.00 to 0.29	Little if any correlation

Table 2.6: Correlation Coefficients

Of interest in my analysis were correlation values where $r > 0.3$, as any lower than 0.3 denotes a negligible correlation for my analysis [121]. In some cases, I have limited this further to $r > 0.5$, so that I narrow my analysis to stronger correlations.

2.2.2 Performance of information security expressed in the context of the 6Ws categorization

This review of the literature was carried out to answer my first RQ1 sub-question (RQ1a) and was designed to identify common **IS Failures** of information security strategies. These show where there are likely to be performance issues in relation to managing IS risks.

Figure 2.4 shows the frequency of node references in the literature. It is clear from this figure that **Human Factors** and **Risk Management** are referenced the most, which was expected. However, Figure 2.5 shows the correlation coefficients associated with success (light grey, upper half) and failure (dark grey, lower half), and this can reveal more important information for my study.

The correlation coefficient values for success and failure for each node are provided in Appendix A. The error bars indicate the standard deviation of all nodes' correlation values. The figure shows that, while **Risk Management** is one of the most frequently mentioned factors (the largest bar), it is mostly attributable to the success of information security, rather than failure. Also, **Architecture** ($r = 0.67$) is the most significant factor of success, and **Internal Threat** ($r = 0.71$) is the most significant factor in the failure of IT security, or in other words, the cause of security incidents. These last

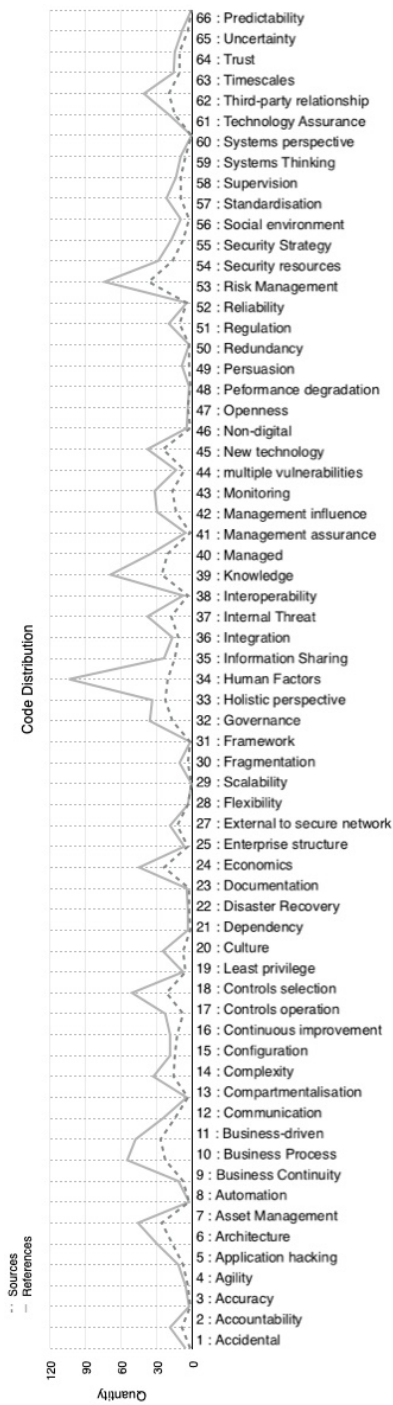


Figure 2.4: Code Distribution

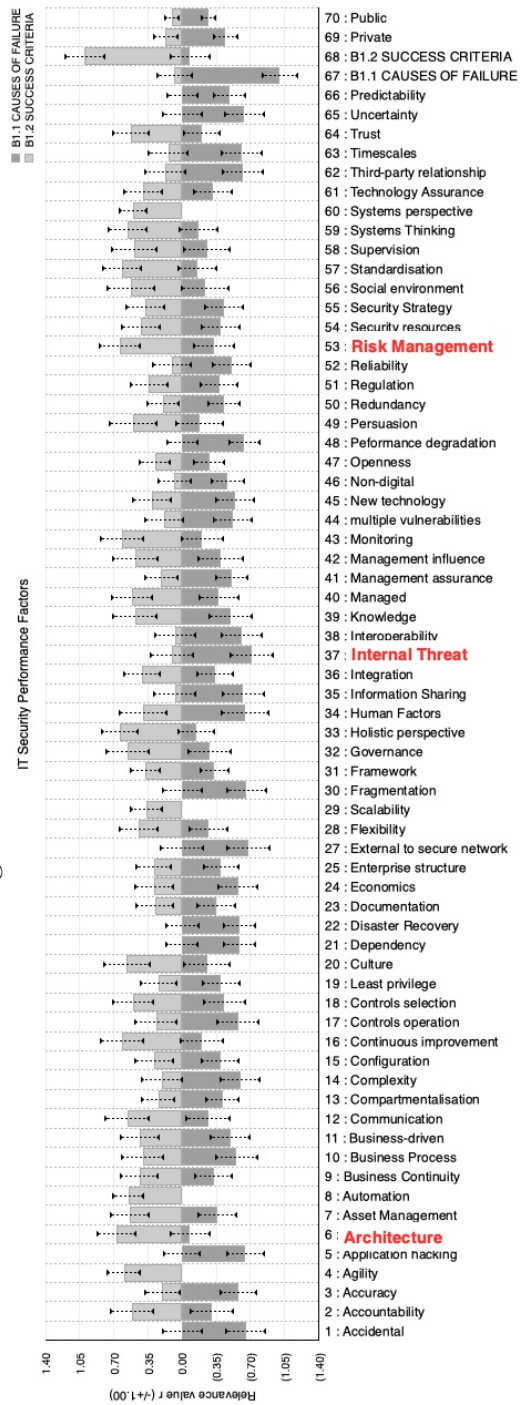


Figure 2.5: Code Correlation with Success or Failure

three nodes have been highlighted in red in Figure 2.5.

It is evident from the above analysis that the success or failure of IT/IS security strategies will depend on many diverse factors. Mukundan and Sai [122] identified that non-IT related factors, such as “asset management, human resource security, physical security, compliance to legal, regulatory and contractual obligation” are equally important as technical factors. Azmi et al [14] concluded that “a multi-prong action is required; one that involves a mixture of technology, competency of manpower, prudence and effective legal framework”. Therefore any study of the security risks associated with an information system should consider the people, processes, and business goals that support the technology [52].

These findings provide further justification for my research on how to assist organizations to take a more holistic approach to information security risk assessments in business change projects. In other words, an approach that should be provided by EAs.

For a first analysis, I arranged the nodes into the most relevant 6W’s category, as shown in Table 2.8. My reasoning at this stage was that this process would help me to align my findings to the structure of some commercial EA frameworks. I eventually discovered that following commercial EA designs was not the right design direction for my artifact (which I describe later), but the 6Ws structure did provide a helpful way to organize and review my findings nonetheless.

6W Category	Node
How	Agility
	Application hacking
	Architecture
	Automation
	Business Process
	Communication
	Controls operation
	Framework

6W Category	Node
	Interoperability Monitoring
What	Accuracy Asset Management Complexity Configuration Controls selection Dependency Documentation Flexibility Fragmentation Information Sharing Integration Knowledge multiple vulnerabilities New technology Non-digital Performance degradation Redundancy Reliability Scalability Standardisation Systems perspective Systems Thinking Technology Assurance
When	Business Continuity Disaster Recovery Timescales
Where	Compartmentalisation External to secure network
Who	Accidental Accountability Enterprise structure Governance Human Factors Internal Threat Least privilege Managed

6W Category	Node
	Persuasion
	Security resources
	Social environment
	Supervision
	Third-party relationship
	Trust
Why	Business-driven
	Continuous improvement
	Culture
	Economics
	Holistic perspective
	Management assurance
	Management influence
	Openness
	Predictability
	Regulation
	Risk Management
	Security Strategy
	Uncertainty

Table 2.8: Nodes grouped by 6Ws categorization

When dynamically creating nodes, I first checked if a suitable node had already been created. However, I discovered that I had created two nodes that essentially mean the same thing: **Uncertainty** and **Predictability**. I treated these nodes the same in the analysis as they were interchangeable and were both associated with failure references.

Also, the **Systems perspective** node was only used once, and after examining the reference, its context meant that I could join this with the **Systems thinking** node in my findings.

I selected, or created, all nodes that applied to the context of the reference, so that I could later analyze the relationships between the nodes to help determine the root cause of failures.

When analyzing the nodes, I categorized my findings into one of the three problem categories that are shown in Table 2.9. These categories identified where problems emerged in the literature. Although they may appear under a specific node, these problems often emerged from evidence across multiple nodes. Also, the problems may not always be associated with explicit references and required decoding using my own empirical knowledge of the issue. For example:

Problem identification: Agreed security controls are sometimes omitted.

This problem identification appears under the node **Timescales**, since that is often a contributory factor, but is also based on the fact that the **Human Factors** node includes references to how people “withhold effort” and “skip security actions”, since experience shows that developers and administrators are just as prone to this human characteristic as end users. Further, **Technical Assurance** was highlighting that technical teams “skip important elements of assurance activities”.

Category	Description
<i>Problem identification</i>	These are specific problems for ISRM that my artifact needs to address directly.
<i>Underlying issue</i>	These are factors that can negatively impact ISRM, so are important to the design of the artifact but probably had to be tolerated rather than changed.
<i>Information</i>	These are additional observations that I wanted to capture for designing the artifact.

Table 2.9: Identification of IS problems in the literature review

The results of my analysis are described below, using the 6Ws as the main categorization and with all 65 nodes providing the sub-categorization.

2.2.2.1 WHY Nodes

Continuous improvement The deployment of new technology is happening at such a pace that vendors do not have enough time to analyze all possible vulnerabilities before the technology is deployed, putting reliance on patching programs [9].

It is important to achieve a careful balance across business and technical boundaries by managing risk, cost, and complexity, so that architectures can respond to the changes in business strategy and policy, as well as regulatory pressures, and evolving threat profiles [29]. Brunette and Scheba [29] describe four transformational phases of “consolidation, standardization, automation, and optimization”. Organizations progressing through these phases will realize the “security, agility, and efficiency of benefits afforded by the systemically secure architecture approach”, thereby increasing their levels of architectural and operational maturity in relation to IT security.

Instead of this top-down approach to planning information security controls and aligning this to corporate risk, many organizations implement security from the bottom-up in a piece by piece process [126].

Underlying issue: Volume of project changes are a risk to security.

Holistic perspective As ISM is multidimensional, a holistic perspective is essential for managing security risks and selecting security controls [52, 149, 172, 131, 31, 81].

State-of-the art technologies, such as mobile and cloud technologies, are changing the business model [31], and the prevalence of mobile communications are risking data leakage [14]. These opportunities create serious risks to organizations, so security managers should take a more holistic approach to information security management and involve senior company executives in decision making. Management play a major role in removing any obstacles, such as budget problems, so need to integrate security with business planning activities [163].

Problem Identification: Senior company executives not formally understanding project risks.

Uncertainty and Predictability There is a level of uncertainty about how systems are measured for their effectiveness. Information and indicators collected for security assessments are never fully credible [162].

As the technological systems grow more sophisticated and complex, so does the security threat, so technological advances both support and hinder information security progress [52].

Security Strategy Information security strategy development should be based on business requirements, and this should be consistent with IT strategy and business strategy throughout the relevant organizational units [106]. It has often been observed that business and technology units tend to focus on delivering their own strategic priorities, and this hinders the alignment of technical and security strategies with the business [30].

Organizational context has a significant impact on the effectiveness of the information security strategy. Therefore, business, information, and technical strategies all need to be in alignment [131].

Business and technology strategies should consider the protection of corporate information, therefore, business strategy and IT strategy should both be aligned with the information management and security strategy.

Underlying issue: Prioritization of work can be unclear.

Business-driven A key influence for information security in organizations is top management support and customer security [122]. Organizations that can demonstrate a reliable and scalable IT-infrastructure are increasingly seen as having a competitive advantage in a cost-aware environment [11].

In a survey conducted in 2013, 85% of organizations stated information security programs were not fulfilling business needs, and 62% stated that they do not align information security to enterprise architecture [79].

Business-led security requirements are seldom followed and are often left to

developers [53]. Despite business and economics determining what technology to use [172], the securing of that technology is then left to developer discretion.

Economics Budgetary constraints are an obstacle to information security management [163]. A lack of budget has been cited as a hurdle for many organizations in relation to information security [79] and cost will always be a factor when making technology decisions [26].

Security controls are not necessarily more secure than the underlying systems that they are protecting [149]. Security software applications could have vulnerabilities that allow them to be exploited by data thieves. Therefore, spending on IT Security that has not been identified as the right solution to a specific vulnerability, could increase the security risks to an organization.

Underlying issue: Budget constraints are a risk to security.

Risk Management Boards need to take responsibility for being aware and prioritizing the management of security vulnerabilities inherent in their strategies [163]. For example, it may be essential for the successful adoption and transition of information systems to a cloud computing environment, that a proactive security risk management framework for the cloud computing environment is implemented [185].

Although risk assessment methodologies can be deceptively simple to use, they rarely provide sufficient detail to assist an organization in making the right decisions when selecting security controls [2].

Complexity increases as the size of the organization grows [162], and so company risk information, such as asset values, threats, vulnerabilities, will always lack an element of credibility. Risk can be managed more effectively when it follows a coherent structure that is linked to the information systems architecture [5].

Any governance framework should be cognizant of other corporate risk governance frameworks and that, “since information security is one of the major corporate risk areas and management of information security risk also should

be a part of corporate risk management framework” [126]. However, corporate risk models may not have a full appreciation of the unique characteristics of the information technology domain, so this needs to be taken into consideration when integrating models, if risk assessments are to be accurately aligned [11].

Whilst Soomro et al. [163], argued the importance of making information security management a part of the business strategy, they also raised the potential shortfall of corporate quantitative risk assessment approaches, suggesting that qualitative approaches that are based on experts’ estimations of potential losses should also be considered.

Problem Identification: Security risk management not expressed in a business context.

Underlying issue: Disparate security and business risk management methods.

Information: Stakeholder qualitative assessments should be considered in risk estimations.

Management assurance Enforcing corporate policy and monitoring compliance is a challenge for organizations [52].

Breaches of security can highlight discontinuities in the management of the organization, and careful consideration of security requirements in IT transformation projects should be enforced [34]. For example, care should be taken when changing employee’s jobs, such as in a reorganization of business functions, to ensure that those affected are still looking after the security of information assets [155].

Problem Identification: Lack of monitoring of security controls.

Management influence Security management should be flexible and support the organization in adapting to new risk environments and support long-term resiliency [52]. Management can positively influence their users by demonstrating good information security practices [122] and by closely monitoring employee behavior [153, 104, 71].

Problem Identification: Management unwilling or unable to monitor compliance.

Regulation Security controls operate well when there is a clear understanding of the information assets, any regulations that must be applied to them, and the risks posed to them [119].

Government-imposed regulations and management responses to that, have a significant bearing on the quality of information security, and this can be negative. Luethi and Knolmayer [112] discovered that high-level regulation had a direct influence on what IT solutions organizations procure and operate. This has resulted in IT services being decentralized and managed between departments and their outsource partners. Whilst these organizations might have good central control of the core IT infrastructure, they were unable to calculate overall system recovery times, and were losing control of information asset management.

Openness Operationally mature organizations are usually self-motivated to respond appropriately to security breaches, and that imposing stricter laws on data security only truly benefit operationally immature firms [149]. When organizations are forced to comply with strict laws, they may be motivated to outsource security services to managed security service providers, in order to meet these laws in a cost effective way. However, in doing so, the risk to information security could actually increase, as the service companies may not be fully focused on the client's risks, and local staff may become overstressed by the focus on compliance [149].

Culture Setting security expectations and defining the security culture begins at the top of the organization [37], and it is the organizational culture that actually influences its employees' behavior [153].

When individuals are not motivated to follow procedures and protect information, security fails [178]. Political pressure (which could be imposed for financial reasons) that forces outsourcing in an ad-hoc manner is therefore

unlikely to provide the organized, in-house regulation (i.e., “keeping a controlling and steering group in-house”) that a successful outsourcing strategy requires [112]. The risk increases when stressful operating conditions exist around IT outsourcing projects. When decisions associated with the outsourcing of IT are made under stressful conditions, this can often lead to human errors [92].

Information: This is likely to be the true influence that management can have. Supporting a good security culture, not dictating it.

2.2.2.2 WHEN Nodes

Timescales The impact of time-related events is seen throughout the articles as a significant factor that is often detrimental to information security strategy.

Collmann and Cooper [34] describe a scenario where a development team perceived itself as using the latest technology to provide new services. They discuss how the team had adopted a fluid work process with few standard procedures. They describe how this was “strong on innovation but weak on established discipline, meeting deadlines for new applications dominated their sense of priorities. They functioned like a “skunkworks” with situation-driven procedures and in relative isolation from other components of KP-IT, particularly Operations”. Whilst the Development team functioned in this very ad-hoc manner, the article also describes how Operations functioned in a more disciplined way but were essentially bypassed and could not have prevented the breach.

Underlying issue: Lack of adherence to security operating procedures.

Problem Identification: Agreed security controls are sometimes omitted.

All too often, the business or economics dictate what information technology will be implemented [172]. Invariably, this contains an element of time pressure, and may not lead to the most appropriate security decisions. In

reality, security failures often lead to greater financial losses and/or further time delays.

It is often the case that development functions are under pressure to meet the demands of business executives [172]. This style of management practice often leaves the development teams responsible for implementing security [53]. Whilst these factors alone increase the risk of security failures, such teams are psychologically driven to shortcut security standards in order to meet the demands of business executives, despite knowing that in many cases the organization has a clear security policy in place.

Problem Identification: Limited understanding of the wider effects of changes.
Underlying issue: High workloads are a risk to security.

Organizations are often exposed to greater risks when they adopt complex and unfamiliar technologies to meet the demands of the increasingly technology-savvy communities [52].

Another important time-related consideration is the increasing speed of exploits to system vulnerabilities. Vendors have to react quickly to fix new vulnerabilities, and user organizations have to respond quickly to applying these security patches [55, 187]. When it comes to technical software vulnerabilities, it is still unreasonable to expect that any organization can patch every vulnerability, as new ones are continuously being discovered [26]. But research has found that attacks increase after the vulnerability has been publicly disclosed [33].

Even the latest technology is being released with numerous vulnerabilities that are placing users at risk [116], and security vendors need to allocate time to reducing vulnerabilities before an IT product ships, by conducting more rigorous risk assessments and product testing [51]. Providing a high-level of product assurance will then gain user confidence and trust, and should ultimately be more economical than developing and implementing patches [33].

Attack vectors are continuously changing and becoming more sophisticated, meaning that security needs to match this pace of evolution [131]. To be

competitive, organizations will need to embrace new technology, extend their capability and replace out-dated systems. Therefore, security strategies and countermeasures should be able to adapt. In effect, information security is a time-related activity, that requires a constant review of threats and vulnerabilities to be effective [9]. Strategies need to encourage a more agile approach to information security [131].

Fenz et al. [55], propose an alternative solution to this problem, by automatically mapping newly discovered security vulnerabilities against the ontological stored IT infrastructure data for the target network, to assess their impact and react semi-automatically or automatically.

Underlying issue: Time-related pressures are a risk to security.

Disaster Recovery When safety mechanisms fail, and security incidents occur, it is important to have trained personnel that can handle the incidents and restore information systems appropriately [140]. This will become more difficult where management has embarked on uncontrolled outsourcing of information management processes, as systems cannot be recovered in a predictable time-frame [112].

Business Continuity The key objective of information security is the continuity of business. Security teams should mitigate the damage caused by security events [84, 140] and adapt to new risks by being flexible [52] in its approach to ISRM.

Information: An enterprise architecture that is set in stone may not be flexible enough to change.

2.2.2.3 WHO Nodes

Social environment Culture cannot be created, but has to be gradually shaped and directed; so whilst security education is important, employees can be influenced by their work environment [153]. Information security in-

cidents can be caused by a disharmony between organizational objectives and social values in an organization, causing users to breach security [4].

People are influenced by the attitudes or actions of their peers, or even the perceived expectations of their peers, so coworker socialization can have an impact on the employee perceptions of information security [71].

Security culture will not be effective if it is not shared by the whole staff, but the socialization process for developing culture might not correlate with the behaviors and attitudes espoused by the organization's management [114].

Information: Development of a good security culture is highly valuable but cannot be commanded.

Supervision Mistakes or violations should be expected and should be actively monitored [104]. It is important to determine if people adhere to security policies and procedures as self-preservation is an instinctive behavior, but information security is not [52]. Therefore, an employee will place work efficiency ahead of security policies.

Waly et al. [178] explain that training and awareness is important but there is limited evidence to verify their effectiveness in a real job environment, so employees need to be encouraged to transfer security training to their workplace; otherwise, security will fail.

Accidental The majority of information security breaches are unintentional and beyond the control of individuals [155]. Given that human error can often occur due to the environment that employees operate in, mistakes are often made in stressful working environments [92].

Breaches can signify broader organizational discontinuities that need to be attended to [34].

Tightly-coupled computerized system architectures can potentially aggravate security mistakes by transforming errors into cascading system accidents [34].

Enterprise structure It has been proposed that information security incidents could be reduced by removing the layers of hierarchy, which is the

cause of disharmony among the less-privileged lower layers of the enterprise [4].

The location of specialized teams involved in information management, technology and security can have a bearing on this. Conflicts between different senior groups of the organization can compromise decisions around information systems [112], so there is an advantage to having information security represented across all vertical structures of the business in a matrix style. This does not mean that there needs to be a security team in each department, but that all departments should have the responsibility for the security of their own information. A central security team can still exist in an expert advisory role but organizations should be wary of any expectation that a central security team can make accurate judgments for all departments.

Problem Identification: Stakeholders not directly engaging with projects.

Problem Identification: Lack of collaboration across separate teams.

Security resources An effective security strategy requires an appropriate pool of competent security professionals to deal with security management tasks. Dzazali et al. [52] highlight that the high cost and lack of availability of suitably competent resources, particularly those with technical knowledge and experience, can make this prohibitive for some organizations.

The responsibility for information security may not be correctly assigned. It is often the case that the person assigned responsibility does not actually have the necessary means to discharge it [52].

The knowledge of security experts serves the organization better if it is documented and shared in a structured way, so that it can be understood and followed by many individuals [3]. Valuable security knowledge is acquired through experience and practice, but if it is only concentrated in a few individuals, then this becomes a vulnerability for the organization. AlHogail et al. describe six main categories of security knowledge: “security risks analysis, security controls, policy and guidelines, standards, IS security tacit knowledge and IS related knowledge”. The latter relates to other corporate knowledge, such as organization mission statement and budget, that is es-

essential for security policy and design.

Essential success factors that are important for information security management are in addition to the security knowledge of the experts, and these include planning, involvement, leadership, organic growth and team work [178]. Good communication between information security management teams and the rest of the business are also essential for an effective information security program [153].

Underlying issue: Difficult to recruit skilled security personnel.

These findings correlate with Figure 2.5, which shows that the work of security specialists has a big impact on the success of IT security when it is combined with other factors, most notably ensuring that their knowledge and guidance is built into a documented way of working for the whole organization. This in turn will reduce the internal threat.

Underlying issue: Security documentation sometimes inadequate.

Human Factors It can be seen in Figure 2.4 that Human Factors is referenced the most in the literature review. An immediate conclusion is that more user education is required. An increase user awareness will help to reduce security risks in most cases [153], but that alone is unlikely to have the desired effect, as this is ignoring aspects of human fallibility.

Whilst technology can help to protect information, such as encryption, this ultimately requires individuals to apply and use the technology correctly [180]. Employees do not necessarily have the same view of information security as management [122] and users may choose convenience ahead of good security practice [65].

Most common types of intentional security breaches are those concerned with the withholding of effort [155]. Users often report skipping security actions, or prioritizing other work ahead of information security practice. This is often because they regarded information security policy to be a hindrance to their normal routine [71].

Mistakes made in routine processes, sometimes described as *slips*, are more common than intentional *violations*, so systems need to be designed with this in mind [104]. Human breaches conform to certain patterns of behavior, which can be identified and protected against, so it is important to monitor processes to identify problems and enforce policy [104]. Management should have a good understanding of how it conducts its business processes to achieve this [136, 104].

Not all unhappy employees will cause harm to the company's information systems [155], but intrusive management can actually have a detrimental effect. More thoughtful monitoring of the well-being of individuals could be more beneficial.

Accountability Employees will be motivated to comply with the perceived wishes of their organization [71]. Whilst published policies and procedures are important, it is essential that organizations know what is actually being followed - what their employees are actually doing [52]. It is instinctive behavior to prioritize self-preservation ahead of preserving and securing information assets. This means that if individuals believe they will be judged more on their results, rather than their methods, they may disregard security policy. Culture plays a very important role here, and that does not happen by publishing policies alone; it comes from the top, by challenging the efficacy of all business processes in terms of meeting those policies.

Poor accountability for information ownership also contributes to unauthorized information asset disclosures, especially to other competitors in the industry [92].

Trust Maintaining good privacy of information leads to trust [115]. Successful policies are those that are actively implemented throughout the organization because they are reinforced and employees have feedback on their performance, and individuals develop self-efficacy as a result [178]. Otherwise, bad habits will ensue, accompanied by a lack of communication, feedback and motivation.

Many organizations are now evaluating another firm's information security

performance when selecting a partner [126], and trusted information sharing solutions will provide assurance for collaboration [33]. Providing a trust mechanism between organizations drove the development of international security standards [102].

Internal Threat Security policies are sometimes constructed without a full appreciation of how the business operates, and this can lead to gaps in the policy, or damage to user confidence, because users simply cannot comply [183].

Problem Identification: Project impact on current business processes not fully considered.

Employee negligence is often cited as the cause of many security breaches [71], but even the most experienced and conscientious individual can slip up and make a mistake, such as opening a harmful attachment or unintentionally visiting a malicious website [33]. Technical controls can certainly help in these instances.

Collusion can occur between an internal fraudster and company employees [51]. The motivation for this is often financial gain, and given the evolving threat profile, all company systems should be inspected regularly to ensure that patches are being applied. This is an example of a relatively simple test for the performance of technical staff, but other aspects of the information security program are less easy to monitor.

Organizations have a challenge in measuring how well information security is meeting its goals [52]. These challenges include: safeguarding sensitive, critical and proprietary information from unauthorized access, disclosure or modification; protecting information systems and supporting computer resources from loss, damage, and destruction; providing organizational management with reasonable assurance as to the integrity, confidentiality and availability of information and information assets; and, recognizing and adopting all legal regulations and laws concerning the confidentiality, availability, and integrity of critical information.

Persuasion Deterrent efforts are likely to positively influence employee behavior if there is a known risk of being caught and disciplined for disregarding security policies [71]. The severity of the penalties can seem less of a deterrent than the risk of being detected. In fact, studies have shown a negative correlation between the size of the penalty and its effectiveness on security behavior [71]. A more severe penalty might reduce the likelihood of it actually being meted out.

When it comes to modifying user behavior, organizations need to influence individuals' security behavior and recognize the importance that peer relations can play in this regard [153]. Staff appraisals may be the right vehicle for any test of individual security performance, and this should reinforce the message that management regard security as a key responsibility for every individual. Cultivating a good security culture within an organization is a long-term strategy, and further research is required into persuasive methodologies that support improving security compliance.

Managed Successful information security strategies are more of a management issue than a technical issue [52].

The numbers of security breaches is still increasing, despite many years of trying to contain the problem, and organizations are bound to continue experiencing problems if they do not manage their security diligently [178]. Whilst the challenges can seem overwhelming, organizational factors are the key barrier to the effective implementation of security policy. Waly et al. list these as: the commitment and support from information security management; conducting assessment of potential security risks and threats; the implementation of appropriate controls to minimize risks and threats; the communication of security issues; planning; involvement; leadership; awareness; organic growth; and teamwork.

Understanding the technical solutions alone is not sufficient, managing information that leaves the digital domain is also important [2].

An outsourcing project should be carefully managed to control how human factors impact information security [92].

Governance Employees may not always know what the organization's expectations actually are [71]. Employee negligence can be a cause of many costly security breaches. Employees can regard security policy as discretionary, and more like guidelines: "employees may choose not to comply with security policies for reasons of convenience in their day-to-day routine" [71].

Most executives regard information security as an administration matter, and have implemented security measures following bottom-up approaches [126]. Ohki et al. advise that executives should be setting benchmarks for acceptability of risks, but, if executives lack awareness of the security risks that they face and what they need to communicate, then it will be impossible for them to achieve a satisfactory level of responsibility. And they are also, therefore, unlikely to assign an appropriate level of resources to manage the risk effectively. How the organization prioritizes the protection of its information assets in a world that is increasingly dependent on information technology, and balances this with business operational need, will also have an impact on the security culture. Security culture should be embedded into the corporate culture to be believed by the organizational workforce and business partners [4].

It follows that if a business change is to be successful, there needs to be a strong understanding at all levels of the organization as to what security changes should be applied to keep business information safe.

Problem Identification: Not understanding the effect of a new system on all personnel.

There is a positive relationship between top management support and the perceived information security priorities [122]. The positive influence and importance of top management support is clear. Left to themselves, employees often underestimate the security risks of their actions, such as transmitting personal information insecurely [122].

The executives of some organizations have been shown to merely pass on government security guidelines to various other parts of the organization to

implement [52]. From an employee perspective it is then clear that the organization is not demonstrating a higher level of information security maturity by defining measurable changes to all business processes and then monitoring compliance from the top.

The quality of executive support and continuous reviews are significant factors in achieving successful information security [163].

Information: Developing a good security culture is ‘part of the whole journey, not a mere destination on the way’ to effective security management.

Third-party relationship The information security performance of third-party organizations should start with the contract – for example: what were the expectations; is this written into the contract; and, are we getting what we ask for? Any review of an organization’s information security posture, has to have due regard for its connections to its business partners, and those partners’ security posture [37].

Unauthorized processing of clients’ information assets is a significant factor in security breaches [92]. One reason for this is the poor control of information ownership responsibility. Organizations are increasingly likely to review the security reports of firms that they intend to use [126]. A positive security attitude to information security is likely to be reflected in their customer’s rating.

Organizations create vulnerabilities by affording contractors excessive, privileged access to client systems when involved in development or maintenance projects [92]. A key success factor for organizations was having detailed security specifications and procedures included during system acquisition and maintenance, with strict access policies for suppliers and contractors [112]. Where these requirements are not standardized, differences can occur across third party working arrangements.

For a long time, organizations have had a need to agree minimum standards of information security that supports the exchange of information. This is precisely the reason why the ISO27005 information security risk management standard was created [102]. However, this is a generic standard that

is designed to cater for most organizations' needs, and therefore requires a consistent risk management method if it is to be implemented effectively.

Lelanne proposes an extension to ISO27005 that introduces the concept of a "service" into the risk assessment process, to help service users ensure that they can maintain controllability of their own data at all times (e.g. what data does the service provider hold, where is that data located, and who has access to it, etc.). Similarly, Zhao [187] suggests that this standard is a good starting point for evaluating the security of cloud services, but also warns that a certification to this standard is not enough to ensure adequate security. The third party's current status needs to be ascertained, and any assurance maintained.

Problem Identification: Insufficient rigor applied when working with third parties.

According to Ohki et al. [126], there can be significant business advantages to sharing information with some business partners, but just one incident could lead to "total business failure".

There are some very important legal considerations for information sharing. Two notable cases of illegal sharing of personal information were raised by Onabajo et al. [128]. One concerned Facebook sharing of consumer personal information with their business partners without the consent of the consumer; and the other concerned Google, for automatically enrolling their Gmail consumers in Buzz, which exposed email addresses and other personal details. The financial penalties for these corporate failings can be very severe. Even when data sharing is kept to the minimum, aggregating several small pieces of data could still allow entities to discover additional information about an individual [103].

But even when the need for sharing information is made transparent to consumers, there are many risks as information is passed from one organization to another. Chen et al. [31], offer an example of an airline industry, where digital data will be delivered to the tour operators, local tour guides, air-

lines, etc., and they determine that an holistic approach to protecting the information is required. They propose three important “axes to build up total shelter, namely: physical environment, data leakage technology, and institutional data protection arrangements”. Even when the transaction is complete, the information could reside in third party systems, increasing the risk of a breach [31]. The entire life-cycle of the information should be made very clear. The arrangements made will not be static guidelines, but should be reviewed and examined continuously to ensure that they are effective.

Problem Identification: Legal compliance reviews not completed for all changes.

Business processes in third party relationships (e.g. through outsourcing arrangements) have redefined the traditional concept of company boundaries [171]. Therefore, an information process in one organization, could impact the information security of another organization, since information security has become increasingly interdependent among those connected organizations. There is a high demand for sharing information outside of the organization’s secure domain, but the threats of exposing data at the perimeter are far greater than within the owning organization’s core IT infrastructure [54].

When operational users are required to access a multitude of separate systems, such as in the healthcare industry, Luethi and Knolmayer [112], found that users often try to save time by sharing system sessions, colleagues’ passwords, or use generic accounts. This problem usually increases when users are accessing systems that are external to their own organization.

Least privilege Whether it is sharing information with a third party, providing access to an organization’s own staff, or simply setting policies for data acquisition and management, the same rule applies: always plan for least privilege principles in the processing of all personal data to support the legitimate business purpose [115, 92].

2.2.2.4 WHAT Nodes

Asset Management Organizations that regard information as invaluable assets consider asset management to be crucial in their security architectures [15]. Categorizing assets greatly assists in this regard, so that controls can be matched appropriately to the asset value [31, 63].

When working on the security requirements for a computer communications architecture, the sensitivity of different types of data should be determined before any meaningful risk assessment can be conducted [26].

Organizations' critical information infrastructure is becoming more massive and intricate and, therefore, increasingly difficult to protect [14]. As cyber criminals become more sophisticated in their attacks and their technical ability grows, so our information becomes increasingly vulnerable to their attacks.

Information: Ensure EA maintenance is not a costly process and is still suitable for lower-value security domains.

Non-digital Organizations' information assets are increasingly residing outside the corporate network (e.g., cloud services) and maybe outside the digital domain entirely (e.g., information copied to paper) [2].

Configuration Secure IT architectures are built in a controlled and methodical manner and are not capriciously designed [26]. Security should be engineered into the architecture at the design stage, where knowledge of the business requirements for security should be understood. Only security measures that are shown to provide financial benefit should be adopted [26].

Organizations can fail to configure individual components securely, leaving them vulnerable to attack [29].

Luethi and Knolmayer [112] question whether a reliance on technical controls for maintaining security is viable for some organizations, particularly where there are heterogeneous systems and cost is an issue. They mention the importance of role-based authorization and single sign-on (SSO) solutions to

enforce security without creating a hindrance for users.

Accuracy Static snapshots of the technical architecture have limited value, as new technology is continually added to the architecture [55].

Cyber security decision makers need to make choices from an holistic point of view but information and indicators collected for security assessments are never credible due to the diverse and complex interconnections across the enterprise [162].

Information: An agile EISA (A-EISA) solution must not enforce the non-essential creation of costly EA artifacts requiring expensive expertise.

New technology An increase in the use of technology often exposes an organization to greater complexities and uncertainties and organizations can be exposed to greater risks when they adopt complex and unfamiliar technologies [52, 34]. Technological change affects how people perform their work duties and consideration should be given to how users are accessing data outside of the scope of the original system design [104].

Strategies that deal with information security threats need to support a dynamic security posture to enable the organization to take swift action in accordance with the changes that are being made to technology [131].

Errors can occur during the implementation of new technology due to a lack of testing [92].

Problem Identification: Ad hoc deployment of new technology.

Scalability A reliable and scalable IT-infrastructure is increasingly seen as a competitive advantage [11]. However, organizations often build components that resolve their internal tasks, and not worry about interfaces [54]. This can lead to differences in architectural platforms.

Standardisation Systemically secure architectures make use of modular, standardized building blocks to ensure that the use of systems is automated,

repeatable, and auditable [29]. Risks should be continually analyzed and as early as possible, so that vulnerabilities can be designed out before code is committed [51].

The use of international standards can contribute to this process but will not provide all of the important security knowledge [3].

Integration Tightly coupled systems can lead to security consequences, such as cascading security breaches [34].

End-to-end security will depend on the coordination of relevant components in the overall architecture [9]. Optimizing security architecture involves deploying the best combination of integrated security technologies [26].

Information Sharing Information sharing may bring huge benefits to an organization but it must be done securely to prevent major security failures [126], as data leakage can happen between the organizations connections [31]. Luethi et al. [112], raise several concerns about relying on point-to-point connections between disparate information systems in order to provide interoperability. Such connections are often achieved through unsecure protocols that lack important security controls, such as secure authentication and auditing.

Interfaces with external systems can be a particular risk. One of the underlying reasons for this is that organizations' priority is often to meet their own internal system requirements, and that the need for interfacing with external processes and organizations is considered as secondary [54]. The result being that it becomes very difficult to add this functionality later in a secure way. Another critical risk factor is the unauthorized access to, modification of, or disclosure of information assets by third parties [92].

Fragmentation Interfacing concerns should be a key consideration for the future-proofing of information technology projects and investments and it is important to avoid fragmentation and provide interoperability of services to avoid copying data out of secure information systems [112].

The introduction of new technology can also compound problems by causing

a fragmentation of responsibility [34], as responsibility becomes transitioned to new online systems with a resulting change in business process.

Complexity It is often difficult to calculate the value of investments for cyber security mechanisms as the level of complexity in an organization rises [162]. For example, what are the real information security risks and how effective is the protection.

There is a need to consider interfaces and inter-dependencies more seriously when conducting risk assessments, as this has been shown to be a significant cause of breaches [172].

Complex, tightly-coupled systems often allow security incidents to spread and escalate [34]. It is difficult for users to spot an error or make any corrections before the error has spread to other systems.

Flexibility Information technology should be flexible to the changing needs of the organization [29], and so the management of security must be flexible to help the business exploit future opportunities [52].

Information: The artifact should encourage the need for future-proofing of solutions.

Multiple vulnerabilities Patching of systems is critical, and organizations must also be aware of the security posture for information sharing mechanisms [33]. To assist in a continual monitoring process, the use of good software tools can be of help [116, 140].

Cloud services may be an effective solution for achieving this in some organizations, as long as they meet the minimum standards required for the specific industry [116].

Systems should be kept secure by making sure that they are well-architected and that valuable data is kept out of reach, e.g., not stored in the clear [65].

Technology Assurance Technical teams may skip important elements of assurance activities, such as formal testing, because they believe this can be

justified as the organization is facing other pressing deadlines [34]. However, organizations can reduce their vulnerabilities by properly planning and managing IT security [149], given that security errors and oversights are often made in the planning and design of systems [9].

Problem Identification: Testing is not completed adequately.

Information: Prototype information security solutions early, to ensure that they are working as expected.

Reliability Reliability and scalability are increasingly seen as competitive concepts [11].

A limited number of technicians keep valuable security knowledge tacit in their own minds, and their effectiveness has been questioned after incidents keep increasing [3]. Systems may not be as reliable as expected [172].

Redundancy Organization should resist introducing single points of failure in their information systems [151], and should ensure adequate load balancing and fail-over is implemented.

Knowledge Methods used for conducting risk assessments can lack sufficient knowledge of the operating domain in question [11]. Therefore greater engagement across teams becomes essential.

Dependency Organizations can become reliant on their information systems to conduct their business, making them increasingly vulnerable to attacks [14].

Controls selection The investment in security controls, such as intrusion detection systems, cryptographic systems and identity management systems, reduce security vulnerabilities, but they may themselves have vulnerabilities [149]. So, just investing in more security controls will not necessarily lower the risk as desired. Systems need to be evaluated carefully before selecting security controls [26].

End-to-end security has to take account of the security of local network components, as well as security in the overall architecture [9]. This can be an issue, as the technical architecture can lack unified planning, and full implementation of existing security products is often lacking [106].

Atighetchi et al. [10] propose a *survivability architecture* that adopts a diverse set of complementary, over-lapping security measures for defense, detection, and reaction, in order to withstand a wide range of threats.

Performance degradation Some security controls can have a negative effect on network performance as they become too restrictive, but additional technology can be built into the network architecture that readdresses the balance [112]. An admirable objective for the resulting physical architecture should be that it is “easy to maintain and the administrative tasks should not be that challenging” [26].

Documentation Security knowledge can be lost with catastrophic results if little documentation is done [3].

Monitoring of systems needs to be formally documented to support an audit process [112].

Systems perspective and Systems Thinking Network security requires a systems perspective [26]. It is surrounded by socio-economic and technical issues in complex system-of-systems, and most IT failures are because of a lack of large-scale, holistic risk analysis and collaborative thinking [172]. Stakeholders need to consider how people are using a system outside of the scope of the original system design, as technological or societal change affects how people continue to perform their work duties [104].

Information: Need to encourage a continuous review of business changes.

2.2.2.5 WHERE Nodes

Compartmentalisation Whilst understanding the complexity of asset management within the organization can be challenging enough, the realization

that not all of these information assets will be contained within the organization's computer systems and networks, further complicates information security [2]. Once organizations' data has left their own environment, those organizations often fail to track that data appropriately.

Organizations build components to solve internal tasks and don't worry about the interfaces [54]. However, a more holistic process is required to uncover threats outside the individual entity [103]. A service-centric view that provides secure enclaves based on least-privilege rules permit more secure communities to share data [29].

Problem Identification: Lack of clarity over information storage and sharing.

External to secure network Despite predictions, paper is still used by many organizations. Once information leaves a controlled digital domain altogether, organizations will have lost even more control of their valuable information [2].

2.2.2.6 HOW Nodes

Business Process The business process is the most important asset of a company, so will come before all other considerations, such as technology [63], and most probably, security.

Engineering information security into business processes is not only important for securing business processes, it can also help organizations to realize greater benefits from their investment in information systems [63].

User involvement is an essential element in building information security into business processes [178], as it highlights the importance of understanding how new technology will be operated in practice. The security culture is manifested in the business processes and activities. Therefore, making information security central to the design of business processes actually reinforces good security culture [4].

Controls might not be operated as designed, or technology could expose new threats that are not adequately protected against [104]. Also, new working

practices could change the way that technology was originally designed to operate. Implementing security technology can be a futile effort if this is not accompanied by clear working practices [52].

Analyzing business assets and processes to identify information flows can determine the most appropriate security solutions [2]. Then, when assessing previously selected controls, it may become clear that they were not the most appropriate. A healthy information management perspective is one that takes an inter-departmental view, and transcends the information security department [34].

Automation The physical architecture for any simple computer network should be easy to maintain and the administrative tasks should not be that challenging [26]. Increasingly, many information security tasks, such as patch management and antivirus updates, are being automated [71]. For securing a complex architecture, automation is an important aspect of maturity in organizations [29]. This allows organizations to capture corporate knowledge and automate business and technical processes at all levels of a security architecture in order to reduce dependency and ensure that processes are consistent and repeatable.

Architecture Conceptual studies on security controls across EA domains, such as security policy, network and access control practices, human resources security, physical and environmental security and compliance, have emphasized the contribution of the each domain's importance in the information security framework of an organization [122]. An effective information security management system should not just focus on technology itself but also the people, processes, and business goals that support the technology [52]. A well-managed enterprise information architecture is critical to the management of information security [163].

Security needs to be developed into the technical architecture [26], and this becomes more important as networks grow and become more complex. For example, even a simple procedure to close out user accounts and adjust access controls ensures good directory management as well as harmonized human

resource and contractor procurement processes [155].

Agility Four transformational phases of consolidation, standardization, automation, and optimization are needed if agility is required in keeping IT architectures secure [29].

Information security countermeasures need to be coupled tightly with new technologies and require continuous updating [131].

Controls operation Most common cause of security breaches occur because of someone “withholding effort”, such as not patching their systems [155].

Also, employees may choose not to comply with security policies for reasons of convenience in their day-to-day routine [71].

Framework International security standards, such as ISO 27001 only provide a baseline and need to be reinforced by frameworks and practical tools [142] to ensure that security planning is matched to business requirements. The development of more tools and frameworks is required so that valuable security knowledge can be built into information security planning [3].

Information: Limitations of international standards reinforces the need for my artifact, as a more suitable metric for ISRM.

Interoperability Many vendors and service providers do not support security interoperability due to a lack of standards [112]. This can result in poor security design around integration of systems and organizations, and provide significant barriers to usability. Tightly integrated services can easily allow errors to flow from one system to another [34].

The role that information security plays in interoperability is usually neglected, but with the growing needs and opportunities in this area, the security risks are increasingly [15].

There can also be a trade-off between providing interoperability and doing this securely [15].

Application hacking The security risk is increasing as hackers’ sophistication and technical expertise increases [14]. Scientific studies have shown that wealthier organizations are likely to be the target of increasing attacks [149]. Attackers may target weaker end points to gain access to core transaction systems [37] and it will be impossible to patch every vulnerability [33]. A significant percentage of breaches occur because hackers are able to introduce malware through vulnerabilities in the systems [149]; Cooper [37] provides an example of a back-end database attack that was staged through exploiting point-of-sale systems in this way. Almubark et al. [4], refer to “unguarded organizations” being susceptible to this kind of external attack, as they neglect to correct deficiencies in their security systems.

Monitoring Organizations need to know whether users are adhering to policies and procedures [52, 71]. Information security is a learned behavior, and assessing individual’s security performance should be the first step to a good security culture [153].

Significant security events should be identified to reduce the unmanaged risks and improve operational security efficiency [81].

Communication Excellent communication between information security officers and staff and stakeholders is the foundation of establishing an information security culture [153]. However, management often believes that merely communicating policies for information security will be sufficient, when in reality, it is only the first step [52].

2.2.3 Performance of Enterprise Architecture

As part of my systematic literature review, I examined the role of EA for assessing information security risks. This specifically relates to the second research sub-question (RQ1b): **EA Role** (see Section 1.5 for details of the research questions). The use of EAs or EISAs is rarely referenced directly in the literature. Where EA was described, it was positively in favor of an architectural approach for implementing successful information security

practices. However, most references to architecture were indirect, in that the literature referenced typical architectural facets, such as the holistic review across enterprise domains, as being beneficial to ISRM.

Architectures help to simplify the complexity of information security strategies in many ways, for example a framework that can easily be followed [131] and for a multi-pronged action [14]. Security should be engineered into every aspect of the network design [26], but future research must not only focus on technology, but should consider the business goals, the processes and people of the organization [52, 163].

Building technology by following a sound architecture makes it easier to understand and support [26]. The architecture itself should be easy to maintain, since it will be constantly changing [55], and should be customized to the specific needs of the organization [163]. An architecture also allows organizations to quickly assess the impact of any new vulnerability discovered within the architecture [55], and helps organizations provide business continuity [163]. The design of Enterprise Information Security Architectures usually starts by identifying the business assets and processes. This is the foundation on which the rest of the architectural layers are built, as this ultimately identifies which security measures need to be implemented [5, 63, 122]. This is regarded as the ‘top-down’ approach, and must consider the full life-cycle of the organization’s information, including third party processing and sharing, and cater for the interfaces that these processes require [54, 126, 163]. In this way, the expenditure on security solutions is easier to justify.

An architecture can make it easier for less experienced personnel to follow good security practices, which can be especially beneficial for small to medium enterprises [3]. Despite these benefits, most organizations have still not adopted an enterprise information security architecture [79].

It can also be seen from Figure 2.5 that the *Architecture* node is mostly attributed to success criteria as opposed to failure ($r=0.67$ for success, $r=0.08$ for failure).

The limited references in my literature review to architecture being a cause of failure were that the documentation is merely “a snapshot in time” [55]

and did not accurately reflect the current architecture. Business departments often focus on their immediate needs only and do not respect the target architecture of the organization [54]. However, these references are not associated with information security failures, they are secondary references to how architecture documentation is viewed in the aftermath of a failure.

Success criteria for *Architecture* references are often expressed in fairly abstract terms, such as how the focus needs to be more holistic in future to consider the organization's people, business goals and processes [122, 52]. This will lead to better judgments about risks and priorities, but it is often directed at larger organizations [15].

This is not to underestimate the value of accurate and up-to-date architecture documentation. A well documented and up-to-date EA gives organizations the ability to determine the potential impact of newly discovered vulnerabilities [55].

Therefore, whilst architecture should be a valuable solution for many organizations, it is not currently stated as a key contributor, or relied upon, to describe how a business functions in reality. This suggests an urgent need for a practical solution to architecture that is more supportive of the current practice, particularly for smaller, leaner and more agile organizations.

My model does not remove the need for good architecture frameworks, but should improve their chances of success.

2.2.4 Difference between Private and Public Sectors

During the systematic literature review, I examined the differences between public and private sector organizations to understand if the sectors identified different problems. This specifically relates to the third research sub-question (RQ1c): **Sectors**.

Referring to the coding of business sector-specific issues shows that there are some clear differences in the security challenges faced by the public and private sectors, and these differences are highlighted below.

Figure 2.6 shows the findings for those nodes which show a correlation

to specific sector references (i.e., those nodes that include a high correlation to *success* or *failure* and also to a *public* or *private* sector distinction). A

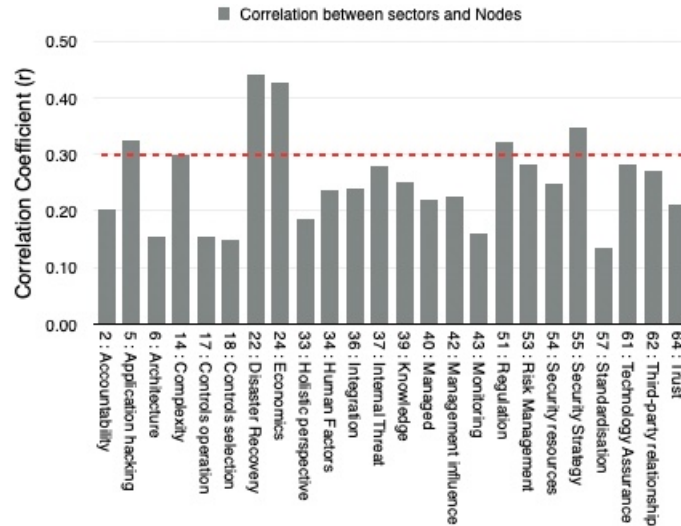


Figure 2.6: Nodes positively correlated with a sector node

table of this data is included at Appendix B.2. The dotted line on Figure 2.6 shows the starting point for any significant correlations ($r \geq 0.3$ - see Table 2.6). Further analysis of the literature identified the reasons for the correlation values and these are described in the next two sections.

2.2.4.1 Security challenges for the Public Sector

Figure 2.6 shows that **economic** pressure is a high factor, and turns out to be one of the strongest differences between the public and private sectors ($r = 0.43$). This is caused by a drain of experienced security professionals towards the private sector [33].

These financial constraints can also directly affect disaster recovery ($r = 0.44$), because there are limited resources available to manage the security strategy and respond to incidents [112].

Regulation is key differentiating factor for this sector, where public sector organizations can be forced to use specific third parties, or bespoke IT solutions [112]. Public sector organizations are also more inclined to outsource some of their security requirements to meet imposed **regulations** in the most

cost-effective way [149].

However, outsourcing to commercial enterprises could increase the risks for a public sector organization, as this creates greater exposure to private sector threats, e.g., **application hacking**, where $r=0.33$ for private organizations. Despite any original claims by service providers, profits can quickly influence their priorities, and take away the focus from the security needs of their existing customers. In fact, outsourcing in the public sector can cause a loss of control of information assets [33], making **recovery** times for those assets uncertain.

Regulations can impose greater levels of transparency on public sector organizations, such as disclosing details of their data breaches. However, these differences can cause public sector organizations to shift their **security strategies** and focus their limited resources into areas of security compliance, and this may not address their highest risks in the longer term. For example, controlling information assets in outsourcing contracts maybe be preferable to implementing a complex technical measure that has been imposed.

Public demands to use information in more innovative ways offered by new technology could further increase the risks for public sector organizations [21], out-weighting internal warnings about the organization's technical or management ability to keep information protected.

2.2.4.2 Security Challenges for the Private Sector

There is usually greater expenditure (reference **Economics**) on IT in the private sector, where this sector attracts some of the best minds in information security, as the career path and salaries offered exceed those in the public sector [33, 112]. However, even commercial organizations can suffer from a lack of coordinated **security strategy**, which can also impact **disaster recovery** in a similar way to the public sector [106].

Application hacking attacks seem to be the largest concern in the private sector [51, 65]. One of the most targeted industries is banking and finance, due to the financial rewards, but there is also concern that parts of

the national infrastructure are now at increasing risk from cyber-attack [33]. Some commercial organizations have placed profit ahead of their customer’s privacy [4], leading to the misuse of personal information for financial gain.

2.3 Exploratory literature review

To obtain key information in relation to my second research question: RQ2 - the **Solution**, the next phase of my literature review was an exploratory review of academic literature for the associated topics that have relevance for an A-EISA solution. These are the areas identified in the yellow associations of the mind map shown in Figure 2.1, and are:

Topic	Reason
Systems thinking	To provide an understanding of system thinking in terms of changing EA domains.
Checklists	My artifact needed to be focused on just the root causes of common IS failures
Agile and Lean Concepts	My artifact needed to support agile business concepts.
Cognitive diversity	To understand the science of involving multiple stakeholders in a security assessment. This topic was identified as part of the ex ante evaluation of early design iterations.
Groupthink	To avoid the risks associated with collective decision making. This topic was researched after reading warnings about consensus decision making of groups (of stakeholders).
Metrics and visualization	To ensure the output of the artifact obtains maximum impact and positive intervention.
Security cultures	To obtain an understanding of how security culture is shaped by the organizational culture.

Table 2.10: Exploratory literature review topics

Human behavioral-science research is an important characteristic of design science research [72], so it was important that I was able to incorporate these attributes into my artifact’s design.

2.3.1 Systems Thinking

The concept of *systems thinking* concerns the holistic review of how the interrelated parts of a system interact. The concept has already surfaced in my EA-targeted literature, but has not been widely discussed. Complex systems, such as business information systems, are non-linear and closed-loop in nature. This means that a small, well-intentioned change in one variable of the system can have a dramatic impact on how the system performs as a whole [61]. Systems thinking provides a perspective of how the components of a system affect each other in various and often unexpected ways [127]. To understand these interdependencies, the dynamic nature of a system should be mapped out to capture its interactions [61].

In agile business change projects, many variables are in a constant state of change. These changes need to be reviewed holistically at an organizational level, e.g., people, processes, contract management, management support, and training, to understand the effects on cyber security risk [143]. Indeed, “security is holistic” [145] and should not be regarded as the disjointed components of a system (i.e., the linear perspective). Savage and Schneider advise that “even a small change to a system can have catastrophic consequences for its security”.

However, there is a lack of focus on holistic approaches to cyber security and technology-centric solutions are dominating strategies for addressing cyber security risks [143]. Salim concludes that this is because of a “lack of awareness and/or unavailability of a comprehensive holistic model for approaching cyber security with a systemic view”. Systems thinking requires a shift in mindset, away from linear to circular. The fundamental principle of this shift is that everything is interconnected.

When following a systems thinking approach for designing a new system architecture, Gharajedaghi [61] explains that it is important to appreciate the environment in which the system operates. Working out the system’s operating boundary is critical to this and requires an understanding of the behavior of its stakeholders. Stakeholders, in the context of a system change, are any individual or group of people that are in some way affected by the proposed

business change. Therefore, they have a stake in its performance. But those with a high *stake* in a system are not necessarily the same people who have a high *influence* on how a project progresses.

2.3.2 The use of checklists

Many organizations are familiar with tracking compliance using standards and maturity models. Compliance strategies are an important requirement for many organizations, but organizations should avoid pursuing security standards which have become disconnected from the risks of their business strategies [142, 149] and find improved ways of keeping pace with business change.

There are many security maturity models that are designed to assess practices against standard criteria, but they have some shortcomings that are problematic for the needs of my artifact. In particular, they do not provide an holistic perspective [93], and often miss the impact of change on human resources. They are also inflexible to rapid change and somewhat overwhelming in their application [85], which makes them unsuitable for smaller, agile projects.

Another consideration for use by my artifact are international Information Security Standards (such as ISO 27001). Whilst these standards are valuable references, they are very generic and abstract in nature [48]. Smaller organizations rarely adopt the complete standard as they can be very complex to manage. Managing too many variables can over-fit the data³ [129] and they are not validated by science and research [158].

A tractable set of questions will help individuals to check the progress of projects in their known environment(s). These questions can provide a repeatable assessment of the most important issues that businesses should consider when assessing information security risks in business change projects, thus allowing the use of the checklist real-time scenarios.

My research had already identified important success factors for ISRM, so my objective was to turn this knowledge into an easy to understand and quick

³Where there is insufficient data to provide a reliable measurement.

to use checklist that focuses on these important factors in business change projects. The final checklist is a set of questions that provide *performance markers* in the CAESAR8 matrix.

The CAESAR8 matrix provides an objective checklist for evaluating information security that is based on scientific knowledge about ISRM. The checklist provides a valuable tool for all project stakeholders [148], regardless of their own security knowledge, and allows the stakeholder to participate in the abstraction of information security risks that can only be identified from their tacit knowledge of their own business area.

2.3.3 Agile and Lean Concepts

My hypothesis was that there would be a greater adoption of EA approaches to ISRM, particularly for SME organizations, if EISA could be achieved in an agile way with reduced time and cost.

Agile and Lean concepts were not mentioned in my systematic literature review, and no corresponding node was created, so my search was purposely kept at a high-level to investigate the underlying values of these concepts, rather than detailed methodologies.

2.3.3.1 Agile

Agile is a method of project management originally used in software development [17]. It involves dividing tasks into short phases of work called iterations. Each iteration is reviewed with the business stakeholders and changes are agreed for the next iteration (bottom-up). This method contrasts with more traditional waterfall developments, where management fully agrees the design in advance of development (top-down). Compared to a top-down approach, agile is better suited to meet the rapid demands of the business, but EA has often been regarded as a top-down process, so agile and EA can be regarded as juxtaposed approaches [32].

Information management and information security can be integrated into common agile software development review cycles [113, 49], which helps to

ensure that security actions for agile user stories are captured on agile dashboards. However, this will not achieve the desire for lighter documentation and faster review cycles [88] or for a move away from the heavy-weight assurance processes required by traditional security standards [19] and some security maturity models. There is a growing recognition that the benefits of an Enterprise Architecture need to be achieved with greater agility [74, 113, 32].

In agile projects, the *Product Owner* is a member of the agile team who is responsible for translating business requirements into project tasks. It is important that the Product Owner understands the business value of achieving the correct security architecture when defining sprints or development iterations [113]. If the Product Owner recognizes that good architecture practice contributes significantly to the business value of the project, and this is repeatedly displayed in early sprints, then incremental steps in a good architectural direction can be made. Even front-loaded, feature-heavy architectural designs in agile are possible in this way [113].

However, an incremental security architecture that defers design costs until features are necessary has also been proposed [32], and this supports the notion of *good-enough* security. This balances the top-down and bottom-up approaches in a way that is supportive of agile, guiding the business and agile teams to develop solutions that meet this concept through growing maturity levels.

Whilst the Agile principles have been established in the software industry and will not always apply to information security projects, the 4 overarching values [17] will always be relevant.

These values represent a shift in focus from the more traditional project approaches and are:

1. Individuals and interactions over processes and tools
2. Working software over comprehensive documentation
3. Customer collaboration over contract negotiation
4. Responding to change over following a plan

2.3.3.2 Lean

Lean is synonymous with the Toyota Production System (TPS), where lean manufacturing principles have made Toyota stand out from its competitors by making processes more efficient and delivering highly reliable products. Lean Manufacturing is a manufacturing paradigm based on elimination of wastes. The lean approach to eliminate wastes is to capture non-value added activities and work to reduce or totally eliminate them [45].

It is stated that Toyota took continuous improvement to a high level by removing waste from the production system [107]. Liker has studied Toyota for 20 years and explains that Toyota's success from 1980 was not achieved by applying a set of statistical tools in a technical way. Its success is derived from creating an organizational culture where everyone, including contractors, is focused on achieving continuous improvement.

Many organizations want to implement Lean to improve their performance but it takes time to develop the cultural shift and embrace the change [20]. However, many characteristics of Lean can be applied when dealing with information security risks. For example, ISRM would benefit from the Lean principle of achieving *flow without interruption*⁴ by allowing ISRM to be seamlessly integrated into a business change process. Another Lean practice that helps with human productivity is having a *collective visualization* [18], by allowing everyone to see how security risks are emerging and being managed.

A well-known Lean concept is Six Sigma. In contrast to the TPS, this is a set of management tools and concepts, and these are focused on process improvement. This is a different concept that was pioneered by a Motorola employee; the American engineer Bill Smith in 1986 [160]. Of particular interest to my research is that Six Sigma aims to remove *variability*⁵ which can

⁴In the context of ISRM, this is the smooth *flow* of operations and information by removing waste, such as waiting times, the creation of unused products or not capitalizing on knowledge [18].

⁵*Variability* is the lack of consistency and is the enemy of manufacturing and the source of performance problems, such as lower throughput and longer lead times [45].

create inefficiencies and impact flow. In relation to ISRM and EA, *variability* could be delays in re-reviewing information risks, finding unacceptable risks too late in a project, or wasting time creating EA artifacts that are not used.

Lean Six Sigma is a combination of Lean and Six Sigma which provides process improvement, but crucially, in a way that also effects organizational culture change. Where these concepts combine, Snee has witnessed a reduction in non-value added work and cycle times [161]. Snee proposes 6 guiding principles for performance improvement:

1. Have a sense of urgency;
2. Review regularly;
3. Understand human behavior;
4. Make it easy;
5. Always have an impact focus⁶; and,
6. Use improvement as a leadership development tool.

These will become important objectives for my research into Agile EA, and will be incorporated into the design goals for my artifact.

Comparison with DMAIC Lean tool. My root cause analysis, which I describe in a later Chapter, identified that CAESAR8 required a second dimension to its checklist in the form of levels. Independent of this analysis, I also noted that a lean tool known as DMAIC compared very closely to the five CAESAR8 levels.

Six Sigma uses a tool for following the improvement cycle used for improving, optimizing and stabilizing business processes and designs [43]. This tool is referred to as **DMAIC: Define, Measure, Analyze, Improve and Control** (DMAIC), which are the five steps for improvement.

⁶This raises an important consideration for the artifact. It should not be used to merely demonstrate compliance, unless this has genuinely been arrived at, but should facilitate investigations into necessary improvements.

DMAIC is a systematic approach for understanding a problem and finding a solution [59] and is intended to help manage changes in the business. The tool has been studied extensively and research has identified how the tool can be used to obtain and share tacit knowledge so that project teams are able to improve their performance and ultimately, project success rates [156].

Table 2.11 shows the two schemes together and these can be read across the corresponding levels as the implementation for assessing information security risks of a business change; i.e., **define** the **business**, **measure** the **change**, **analyze** the security **impact**, **improve** the security **strategy** and **optimize** security **controls** for future resilience.

level	DMAIC	CAESAR8
1	Define	The Business
2	Measure	Business Change
3	Analyze	Security Impact
4	Improve	Security Strategy
5	Control	Optimization

Table 2.11: The 5 Levels

Given the success of *Lean* in business [107], this comparison indicates that the results of my analysis into CAESAR8 levels should be relevant as a practical tool for businesses.

2.3.4 Cognitive Diversity

The study of how different individuals poses a different *cognitive set* from which to approach problem solving is called *cognitive heuristics* [35]. A heuristic allows people to quickly arrive at a judgment based on their specific inner knowledge and experience of the subject matter and this makes up their cognitive set. This bringing together of different perspectives is an important aspect of *knowledge representation* [35], to improve the quality of decision making. Page has studied the benefits of diverse group composition

in problem solving [75] and refers to this specific collection of cognitive psychology as **cognitive diversity** [129].

CAESAR8 needs to be designed to provide an enterprise perspective of change risks, and therefore captures this *distributed cognition*. Distributed cognition explains how organizations are able to achieve complex business processes successfully (e.g., by dividing up sub tasks to experts) and is also relevant for assessing the effect of change programs. The full set of collective knowledge and perspectives should be obtained from the parts of the business that are affected by the change program. My artifact assimilates this information in the same way for all stakeholders involved in the project to create a single, shared picture of risk - a collective visualization [18].

Introducing cognitive diversity allows groups to arrive at better judgments [129]. Page describes cognitive diversity in terms of the differences in people's knowledge and experience, including information, knowledge, heuristics, representation, and mental models. Whilst security experts can play a vital role in defining security strategies and reviewing business change, there is a danger in relying on individual experts when assessing security risks, as one individual may not have the complete awareness of all corporate issues that a group of business stakeholders might have collectively. Relevant stakeholders are likely to have a practical understanding of how their respective parts of the business are affected by a change [129], whereas a security expert may only have basic information on which to pass judgment. For this reason, "diversity trumps ability" [75], as solutions to complex problems often require multiple points of view. More diverse perspectives deliver a better overall solution, as long as each individual brings relevant knowledge and perspectives.

Individuals, or homologous groups, can show an under-reaction or over-reaction to new information when considering threats [8]. As a result, organizations that rely on a single expert's judgment may accept a level of subjectivity in decisions as a result of untreated biases [159]. Experts are also more prone to miss alternatives than lay people and can treat their preferred models as infallible [159]. Also, when posed with a question, experts

have been shown to substitute similar alternative questions for which they already have a familiar response [86].

An expert's intuitive judgment is therefore prone to errors and biases, meaning that their judgments may be made with a misplaced level of confidence [87]. Moreover, the quality of an expert's decision making rarely improves with experience, partly due to limited opportunities for feedback [94]. Further, experts are not always consistent in their judgments. This can be because of venality, where experts take positions that serve their immediate self-interests [123], but also because of other biases such as *cognitive dissonance*, where an expert's overarching belief may overpower their concerns with the specific issues under review. As a result, even the same expert can make a different judgment on a different day.

Therefore, the opinions of a knowledgeable, diverse group of experts who offer different knowledge, perspectives and heuristics [75] are important for the design of my artifact. These will be people who share a common goal in the project but who also offer different perspectives or skill sets, so are likely to employ a different mode of thinking.

Another benefit of CAESAR8's design to capture the diverse knowledge of project stakeholders is that it also captures their tacit knowledge. I define *tacit* knowledge as knowledge which has not yet been articulated or cannot be articulated [70]. This is the opposite to *explicit* knowledge which can be articulated, and in the context of EA, is usually articulated in EA artifacts. These EA artifacts usually provide written descriptions of an organization from different perspectives. However, tacit knowledge is information that stakeholders subconsciously know from their specific awareness and/or experience. In the context of EA, tacit knowledge could relate to an awareness of how an otherwise unconnected part of an organization's operations might be indirectly affected by a change. Although the interactions of these different parts of the business may not be written down, a stakeholder is likely to instinctively *know*. These are matters that cannot be committed to 'stone' in EA artifacts.

My artifact needs to fully understand how these business change projects will

impact all business functions before and after the change. My solution to the problem of accessing the relevant tacit knowledge of affected departments was to require an in-person assessment from all the key stakeholders involved in a project. Because agile projects are very fluid, with repeated iterations making constant changes, the assessment would need to be repeated for each iteration of a change project, so needs to be a quick and easy process.

2.3.5 Groupthink

The term *Groupthink* refers to the mode of thinking that persons engage in when concurrence-seeking becomes so dominant in a cohesive ingroup that it overrides realistic appraisal of alternative courses of action [82]. It is therefore important to avoid creating groupthink scenarios.

The sense of conformity (this is a *request*, and is different from obedience, which is an *order*) can be so strong and powerful for an individual, that it subconsciously overrides their own thoughts to the contrary. This overriding sense of conformity has led to disasters across industries. For example, in the aviation industry, co-pilots have chosen to risk death, rather than contradict their captains [120]. In medicine, junior health care staff have failed to speak up about concerns with their supervisors' patient management plans [168]. Working in groups can also lead individuals to increase their risk taking. This *Illusion of Invulnerability* is a consequence of groups making judgments together [82, 69]. Therefore, it is vital that security risk assessments are conducted independently, so that stakeholders are permitted to inform the overall decision without undue influence.

For the reasons of avoiding groupthink, my artifact needs to provide this independence of judgment.

2.3.6 Metrics and visualization

A key requirement for any A-EISA solution is to share the process across teams and communicate to corporate decision makers. This is important for achieving the *collective visualization* that I describe in my earlier section on

Lean principles, Section 2.3.3.2.

I identified many attempts at providing useful metrics in the literature, such as new models to calculate the probability that attacks will succeed and the expected loss [162], the significance of measuring time elements [124], and financial investments [25]. However, many of these attempts were dependent on quantitative approaches that have a heavy technical bias [60], and are often based on linking to commercial standards, such as ISO 27001, to match control objectives to vulnerabilities [28], or attack/defense scenarios [133]. Aggregating the dynamic status of information systems to a single metric loses essential information but conversely, specifying too much detail makes it difficult to determine relevance [134]. Furthermore, applying security standards in a serial order is unlikely to protect against the full range of vulnerabilities that an organization can face, and will not consider realistic, dynamic attack scenarios.

Where a competitive advantage is important for organizations, benchmarking information security key performance indicators (KPIs) against other organizations can be a valuable indicator, and where barriers to protecting such information exist, privacy preserving benchmarking solutions have been described in the literature [91, 181, 186]. However, accurately specifying static evaluation metrics that will measure security posture for even the most similar organizations have still not provided a means of providing reliable comparisons [65].

Whilst these are valuable studies, my early conceptual models had led me to conclude that a simple “Go” / “No Go” decision is the most suitable for management, based on the results of assessments conducted by knowledgeable stakeholders. Therefore, a familiar and simple traffic light rating system, that shows a Red, Amber or Green status, might be sufficient (sometimes referred to as a RAG system for this reason). This is a common rating system used in project management to show where work is either on track or at risk. An *Amber* status indicates that work had started in a particular area but was not yet complete.

Axelrod [13] describes this type of metric as *Existence Metrics*. This study identifies that these type of metrics are useful for providing high-level indi-

cations as to the security posture of an entity [13].

Using these nominal category values for my artifact provides an easy-to-interpret visualization of potentially complex risk scenarios. The resulting dashboard is quick and easy to communicate to senior executives of an organization.

This is not an area that has been covered extensively within academic literature. One of the limitations of this category of metrics is that it can lack granular detail, such as quality and completeness [13]. However, a study has shown that summarizing project risks in this way, based on accurate assessments, and reporting issues over time, will present management with a valuable prediction about where projects may be running into trouble and when intervention may be required [76].

My artifact depends on individual experts providing their assessments at this higher level, but it should be backed up by whatever detailed assessments a stakeholder deems necessary. Any concerns identified at a detailed level would then be summarized and reported through the model to provide a shared perspective of risk. For example, if a security expert knew that the firewall rules needed reviewing/updating following the change, they may decide that their assessment for the technical security impact or security strategy is no higher than “Amber”, thus determining the current status of the consolidated assessment. My artifact should therefore be considered as the *high-level indication*, i.e., the top of a hierarchy [146], that provides an important visualization of the security posture of a change project and allows experts to drill down to their own specific stakeholder metrics.

The presentation of the metrics must still meet the needs of the intended audience. A radial format is shown in Figure 2.7, next to a matrix style visualization of the same data. Matrices are commonly used for presenting the results of risk assessments.

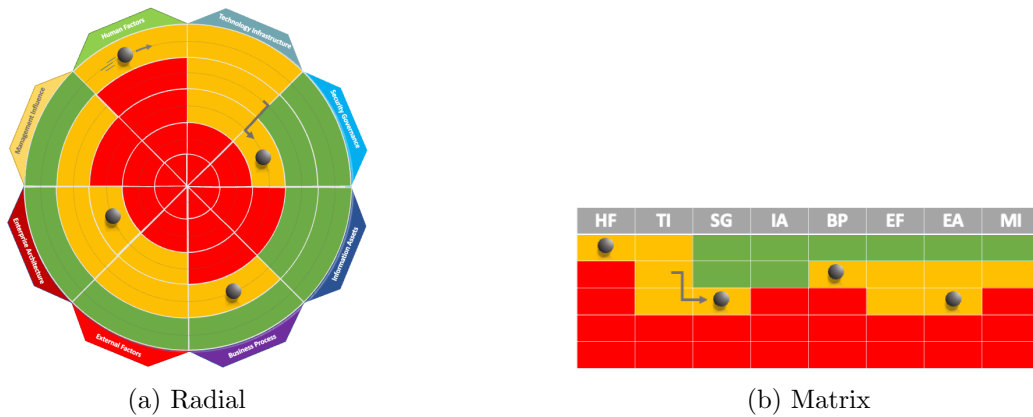


Figure 2.7: Different visualization formats

The small gray balls (which I refer to as *electrons*) in the figure represent where stakeholders are making the latest changes to the model. It can be seen how the radial style supports the notion of continuous assessments (depicted by orbiting electrons), whereas the matrix style gives the impression that the assessment will be complete on reaching the right hand side of the matrix.

The radial format offers a number of advantages for reading the results of the assessment. Of particular relevance is the centroid (center point) of the radial visualization [50]. For a “Go” / “No Go” decision, where senior executives maybe analyzing the graph and deciding whether to launch a new system for example, mature projects should have turned the figure green by progressing to the point in the center of the figure. The centroid logically denotes the end of the assessment. For the CAESAR8 model, the center is level 5, which is only important for optimizing a solution. This is significant because the center ring is the smallest and will naturally be regarded as the less significant [47] - which for CAESAR8, will be true

Progress across the eight domains is more critical than achieving levels. The levels are only significant for achieving the domain requirements in the correct order. Studies have shown that radial diagrams offer the best format for presenting progress in primarily one dimension [47] and that this is read more accurately if this dimension is displayed in sectors as opposed to the

rings [47, 62]⁷. This quality of radial diagrams to highlight the symmetry across sectors (the domains) as the assessment moves between the levels [62] is an important benefit. Although it is easier to read the results across two dimensions in the matrix diagram, the prominence of the second dimension detracts from the more important first dimension. This effect is noticeable in Figure 2.7, where more domain patterns are immediately noticeable in the Radial, compared to the Matrix.

The matrix format also provides a clearer visual for a quantitative dimension (i.e., what level each domain has reached), but this is not relevant for CAE-SAR8, where a level is only *reached* if all domains have reached it together. Finally, for the purpose of rapid reviews of project iterations, the radial diagram will be quicker to read as it results in a reduced distance for the eye to scan [176]. This will become an advantage when discerning temporal patterns between more than one consolidated set of results for the purpose of judging progress.

2.3.7 Security cultures

The security culture within an organization describes how information security is embedded into the decisions and actions of its employees. I have already discussed how the use of EAs can often be directed to technical matters, but the biggest impact on information security is the human dimension [4].

Whilst introducing security controls, such as security policies and awareness programs is important for creating a good security culture, it is necessary to understand that organizational culture will impact the effectiveness of the security culture. Acculturation is defined at the top of an organization [52] and governs how the company conducts its business. If the executive simply mandate a good security culture in corporate policy but that policy is not reflected in the way the business is directed, then a good security culture is unlikely to be achieved [178]. Without effective enforcement, the security

⁷Although if a user wanted to read the second dimension, it is only five levels, so can still be read accurately.

culture is likely to be influenced more by the social environment in a way that is not planned or expected [114, 71]. The effect can be greatest in smaller organizations, where employees are more exposed to external influences [111]. Da Veiga and Eloff [40] propose an Information Security Culture Framework (ISCF) that assists organizations in developing the right security culture. The ISCF works across three tiers of the organization: i) organization tier; ii) group tier; and iii) individual tier. Whilst security awareness, for example, will impact the individual, it is important to think of employees as being members of groups [40]. Business change programs can often present a problem for information security as employees can be resistant to change [111]. However, for a business change, the ISCF defines how organizations need to consider how holistic changes need to be made in the group tier, such as its operations and monitoring, to accommodate the change correctly and maintain a good security culture.

The role of middle management (within these group tiers) is critical for integrating security into the organizational culture [38, 174], and it will require careful management of employee actions. Therefore, middle management should know and understand all of the business processes that they are responsible for and ensure that corporate values from the top can, and are being, maintained throughout all business change initiatives. If employees are not motivated to follow the correct security practices, then a good security culture will not be achieved [178, 51]. For example, if elements of an organization's digitization transformation program involve the outsourcing of information processing, the affected stakeholders must review how that impacts their responsibilities for managing their information. Evidence of a security certification from the cloud provider obtained by the security team, for example, will not constitute sufficient due diligence.

This means that stakeholders who represent their departments can make a significant difference on the security culture within an organization and this is exactly why CAESAR8 has been designed to provide holistic assessments of business changes in the middle tier. Stakeholders should be asked for their opinions and perspectives on security matters and must be supported to express their views freely.

A security team will probably not be in a position to judge the full impact of a change if they are only basing their decisions on a perception of how a process *should* work. The ability for security professionals to involve key business stakeholders in the CAESAR8 assessments in a *bottom-up* process is key to achieving a more accurate assessment of how the security culture will be affected by a business change.

2.4 Search for similar artifacts

My systematic literature review did not identify any specific frameworks, models or tools for an A-EISA or an agile EA, so I conducted separate searches for similar artifacts. These searches are described in Table 2.13.

Search #	Db	Keywords	Result
1	Scopus	KEY (risk) AND KEY (architecture) AND KEY (“information security”) AND KEY (model OR tool) AND KEY (agile)	0
2	Scopus	KEY (risk) AND KEY (architecture) AND KEY (“information security”) AND KEY (model OR tool)	19
3	Scopus	KEY (“information security”) AND KEY (“risk assessment”) AND KEY (stakeholder)	5
4	Scopus	KEY (“enterprise architecture”) AND KEY (stakeholder)	50
5	Google Scholar	‘information security’ and ‘risk assessment’ and ‘model’ and ‘stakeholders’ and ‘enterprise security architecture’ and ‘agile’	...

Table 2.13: Search strings for finding similar artifacts

2.4.1 Explanation of search results

Search #1 was designed to identify agile tools for EA-based ISRM but this search returned zero documents.

Search #2 removed the keyword “agile” from search #1 and this returned 19 documents⁸ but none of the articles presented an existing model or tool. The results included research that confirmed the integration of Risk Management (RM) and EA was beneficial to ISRM [46] but no designs for a model that provide organizations with a practical EA-based solution were included.

Search #3 was conducted for information security and risk assessment without requiring the architecture element. A key contribution of my research is obtaining the involvement of stakeholders for ISRM. Therefore, this search also included the keyword, “stakeholder” to make sure that the results provided this perspective. It only returned 5 documents and provided no examples of a model.

Search #4 was conducted to find EA articles that included “stakeholder” perspectives in the context of EAs, and this returned 50 articles. However, many of the most recent articles in this search result related to the difficulties in obtaining and maintaining stakeholder involvement.

The search highlights that a successful EA implementation in an enterprise requires committed engagement and active participation from stakeholders, but stakeholders can view EA content (EA artifacts) as too complicated [138]. Even the most current research in this area recognizes the problems of stakeholder engagement and proposes many theories about how stakeholders are prevented from participating in EA [101]. Many of these problems were identified in my research and form the basis of my formal problem identification.

⁸Checked on 20/05/2021.

Search #5 returned an article that confirmed the benefits of using an enterprise architecture approach for conducting risk assessments on new IT services [144]. However, this article also highlights the potential limitations of using an existing framework, in this case specifically SABSA [154], for maintaining currency of enterprise risks in a constantly changing organization.

Search #5 did identify a useful literature review for research into ESA frameworks and was based on the following research question: “will a holistic security model using EA provide security benefits to an organization more effectively than a piecemeal approach” [117]. In the article, McClintock et al. describe how they have recently researched 25 security models and have determined that an holistic approach to assessing information security risks is beneficial.

This study is clearly relevant to my research, however, they determine that none of these models consider all aspects of information security equally, namely “information, physical, technical process, people, cycles and risk”. They determine that a new model should be developed, and propose a new model based on the Zachman Framework [184] but tailored to the holistic needs of information security management. The authors call this model “Security Architecture Framework for Enterprises (SAFE)”. I discuss this specific model in the next section.

2.4.2 Discussion on the SAFE model

The SAFE model uses the same matrix that is used by the Zachman Framework [184]. SAFE is similar, but less technical, than the SABSA framework [154], which is also based on the Zachman Framework matrix. I show this matrix in Table 2.5.

Like SABSA, SAFE does not embrace agile principles. Whilst SAFE may offer an improvement by conducting ISRM within an EA context, it is still based on a commercial EA framework that may lack evidence of delivering the intended benefits to a business [97]. This is particularly relevant as one of the principles that the authors quote is that SAFE should be completed for

the whole organization. McClintock et al. identified 4 principles for SAFE:

1. The purpose of an effective framework should be to support the organization's vision;
2. An internationally recognized standard should be used to provide a security assurance to the framework developed;
3. The framework development should be based on EA; and,
4. The development of an ESA framework should be a focus for the whole of the organisation, not just singular departments or assets.

These principles have been developed from the analysis of existing EA frameworks. This approach could limit the scientific value of the principles derived, since the analysis will be based on a commercially-driven perspective of EA. For example, it has led to the modeling of the entire organization (principle 4) and mapping to an international standard, such as ISO 27000 and NIST (National Institute of Standards and Technology) (principle 2). However, my research has found limited evidence that the business benefits of commercial architecture frameworks or international security standards are based on scientific evidence [97, 158, 48].

McClintock et al. present their risk management configuration cell as an example for the reader. This is a very important component of the framework but this article offers an example of a commercial matrix-style of risk assessment. I have already described how this may potentially introduce a subjective judgment of risk (see Section 1.2 of the Introduction).

Further, one of the challenges that the SAFE model may have is its complexity, and this is also true for the more traditional EA frameworks on which it is based. This was a view that was expressed by participants in their evaluation of SAFE, and their analysis determined that these comments were made by people with less security knowledge. This is a key point that my artifact is designed to address, as a novel feature of my artifact is the total involvement of non-security stakeholders for holistic risk assessments for the organization.

Therefore, whilst my study concurs with SAFE's principles 1 and 3, I do not consider that principles 2 and 4 will be appropriate for the design of a practical EA-based artifact. Particularly so for an agile EA solution, as principles 2 and 4 will limit the adaptive ability of the model.

Whilst none of the twenty five models that McClintock et al. reviewed in their study offered the same or similar functionality as CAESAR8, one the models, called PFIREs: A Policy Framework for Information Security [139] follows a similar cycle. I conducted a respective review of this model and explain its similarities in the next section.

2.4.3 Discussion on PFIREs

In many respects, my artifact follows a similar cycle to the four phase model developed by Rees et al. in 2003 [139]: PFIREs: A Policy Framework for Information Security (see Figure 2.8). The PFIREs life cycle consists of four major phases: Assess, Plan, Deliver, and Operate. Each phase has defined exit criteria that should be met before transitioning to the next phase. These phases are similar to CAESAR8 levels.

However CAESAR8 provides a far greater depth of analysis, which was a limitation that Rees et al. proposed future research should address. Although the PFIREs model is relatively high-level and only represents the overarching concept of my artifact, it does describe the cyclical nature that an agile EA approach will need to adopt to meet rapid changes in business risk. Whilst traditional EA Frameworks often provide the depth, their focus can be too broad and their implementation too linear. They cannot easily adapt to changes in the business [88, 96].

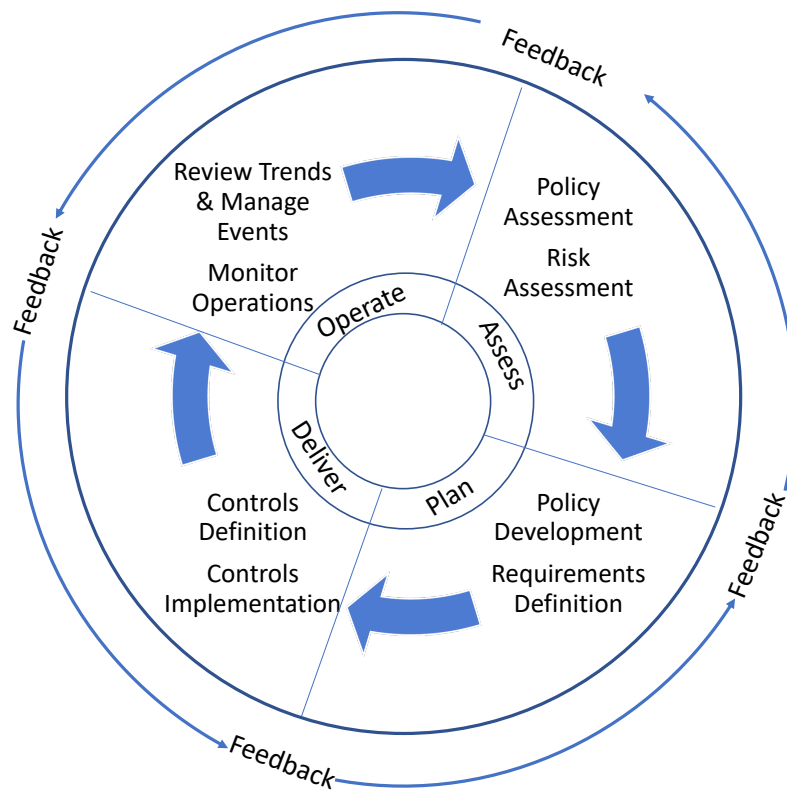


Figure 2.8: My interpretation of the PFIREs Four Phase model [139]

2.4.4 Theories for the EA discipline

My literature review identified discussions on how improvements might be made to address EA and EISA problems. One useful article provided a scientific analysis of empirical studies on the practical usage of enterprise architecture artifacts in multiple organizations [98]. Kotusev et al. have identified 10 theories that can be considered key for understanding how an enterprise architecture practice works. The authors explain how the EA discipline has largely been atheoretical in nature and articulate a practical purpose for these theories, which offer EA practitioners corresponding guidelines when working with EA artifacts. These are described in Table 2.15.

Theory	Analysis	Practice
Boundary objects theory	Describes the usage of EA artifacts for communication between business and IT stakeholders	Create EA artifacts providing relevant information to all their business and IT stakeholders, addressing their needs and helping align their interests
Actor-network theory	Describes the usage of EA artifacts for communication between different organizational levels	Establish concrete enforcement mechanisms (e.g. formal governance, peer review or direct supervision) for all EA artifacts reflecting certain planning decisions to ensure that these decisions are taken into account during decision-making processes somewhere at lower organizational levels
Cognitive fit theory	Describes what presentation formats in EA artifacts are suitable for different tasks	Align the information presentation format and structure of EA artifacts to the nature of tasks, problems and decisions that these artifacts are intended to support, make sure that their format is convenient for decision-makers
Information processing theory	Describes the fact that complex EA artifacts are not used for decision-making purposes	Simplify all EA artifacts intended for decision-making purposes, focus only on the most essential information critical for decision-makers, organize information hierarchically with only a limited number of significant elements at each level of the hierarchy
Uncertainty principle	Describes the fact that global, long-term planning is supported by very abstract EA artifacts	Develop EA artifacts using adequate abstractions appropriate for the affected organizational scopes and planning horizons, avoid attempts to describe the distant future in every detail
Communities of practice	Describes the place and usage of EA artifacts in the organizational social landscape	Establish periodical meetings engaging representatives of different groups of stakeholders and also design complementary EA artifacts to facilitate these meetings, but avoid over-reliance only on one of these two approaches

Theory	Analysis	Practice
Knowledge management theory	Describes different usage of EA artifacts capturing IT landscapes and business visions	Do not try to document everything in EA artifacts and do not expect to find all the necessary knowledge there, in complex situations and questions seek direct conversations with competent people, include in EA artifacts the lists of their contributors so that these people can be easily identified and contacted when necessary
Media richness theory	Describes different communication patterns for EA artifacts reflecting opinions and facts	Seek direct face-to-face meetings with relevant stakeholders for developing EA artifacts that imply significant planning decisions to minimize the chance of misunderstanding, avoid attempts to discuss the desired future via electronic communication media, for example, emails, corporate portals, wikis, and chats
Decision-making theories	Describe the participation of stakeholders in the creation of future-focused EA artifacts	Involve all their stakeholders into the development processes of EA artifacts defining the future course of action, avoid attempts to make planning decisions on behalf of their real stakeholders
Management fashion theory	Describes dramatic differences between recommended and actual usage of EA artifacts	Understand that all prescriptive step-by-step EA methodologies and popular EA frameworks is only a management fashion actively promoted by fashion-setters, do not try to implement their recommendations in practice

Table 2.15: 10 Theories for EA research

Kotusev et al. do not describe agile considerations and their research also relates to the broader use of EA artifacts, rather than information security specifically, but their guidelines are valuable for EA in practice. Whilst the design of my artifact was at a mature state when this article was published, it nevertheless serves a valuable document for validating my research.

2.5 Conclusion of Literature Review

In this chapter I have explained how I conducted a systematic literature review to provide intelligence gathering to answer my first research question (RQ1), e.g., why do certain ISRM initiatives fail. I then conducted exploratory searches of the literature to answer my second research question (RQ2), i.e., how to design a more practical, agile EA approach to ISRM.

To ensure that my systematic literature review was not limited to existing EA research, I divided my search into two parts: i) to analyze all causes of ISRM failures (regardless of any EA involvement); and ii) to research how EA approaches impacted ISRM specifically. This provided details of EA in the context of ISRM, and it also provided valuable data for later analysis in my DSR process.

Whilst I discovered that EA approaches theoretically provide an holistic solution for IRSM, no specific frameworks were described. I later discovered that commercial EA frameworks do not necessarily provide a sound scientific basis for a practical solution for IRSM. As an example, I documented my findings of the literature review in the context of the six interrogative questions common to some commercial EA frameworks (How, What, When, Where, Who and Why). However, this proved not to be a good fit for the data that I discovered in the literature.

At the end of my systematic literature review, I had identified fifteen problems that an ISRM solution must address. In addition, I discovered that there are underlying issues that need to be considered during the solution's design and development (DSRP Step 3).

As I possessed empirical knowledge of ISRM, I found that dynamically coding the literature, rather than be constrained by a predetermined coding structure, meant that I was free to record all issues found. Having a single researcher conduct the coding in this way was beneficial as it didn't require coordination.

My exploratory literature search provided valuable research into behavioral-

science, which I used in design-science to create the novel CAESAR8 model. The work carried out by other researchers on the Information Security Culture Framework (ISCF), for example, highlighted to me the significance of reviewing business changes with the business groups affected, which is a significant feature of the CAESAR8 model.

Table 2.16 summarizes how my literature search provided key research for the design and development iterations of the artifact. Also shown is the search type in relation to the original search plan (see Figure 2.1).

#	Search Type	Description	Section
<i>1st Iteration</i>		<i>(Cyclical model design)</i>	
1a	Systematic	Problem identification and objectives	2.2.2
1b	Exploratory	System Thinking	2.3.1
1c	Exploratory	Agile values for artifact design	2.3.3.1
1d	Exploratory	Lean concepts for artifact design	2.3.3.2
1e	Exploratory	Metrics and visualization	2.3.6
<i>2nd Iteration</i>		<i>(Final concept CAESAR8 model)</i>	
2a	Systematic	Quantitative analysis of node influence	5.1
2b	Systematic	Qualitative analysis identified domains	5.2
<i>3rd Iteration</i>		<i>(First prototype CAESAR8 model)</i>	
3a	Exploratory	Checklists	2.3.2
3b	Systematic	Pairwise analysis of strong correlations identified key IS issues	5.3
3c	Systematic	Pairwise analysis identified Maturity Levels	5.4
3d	Systematic	Chains of influence identified Performance Markers	5.5
<i>4th Iteration</i>		<i>(Combining assessments)</i>	
4a	Exploratory	Organizational and security cultures	2.3.7
4b	Exploratory	Cognitive Diversity	2.3.4
<i>5th Iteration</i>		<i>(Multiple stakeholders perspectives)</i>	
5a	Exploratory	Groupthink	2.3.5

Table 2.16: Literature review associated with design iterations

Chapter 3

Research Methodology

The aim of my research was to make a contribution that moves EA from the theoretical realm for many smaller organizations, into a practical solution. To address my second research question of “*how can organizations adopt a more agile approach to using EA in information security risk assessments*” (RQ2 - the Solution), I decided to select the Design Science Research methodology to design a novel artifact that is based on scientific research, including an evaluation by industry experts.

Following this applied methodology has allowed me to design a practical solution, a process model, that combines existing areas of behavioral-science research to solve a practical problem in the business target domain. The resulting artifact provides a pragmatic solution that organizations can use to improve the human performance in the field of ISRM.

3.1 Design Science Research Approach

For my design science methodology, I have followed the Design Science Research Process Model (DSRP model) [132]. The DSRP model consists of 6 steps, which are all followed in the research. These steps are summarized in Figure 3.1, and are: Problem identification and motivation, Objectives of a solution, Design and development, Demonstration, Evaluation, Communication.

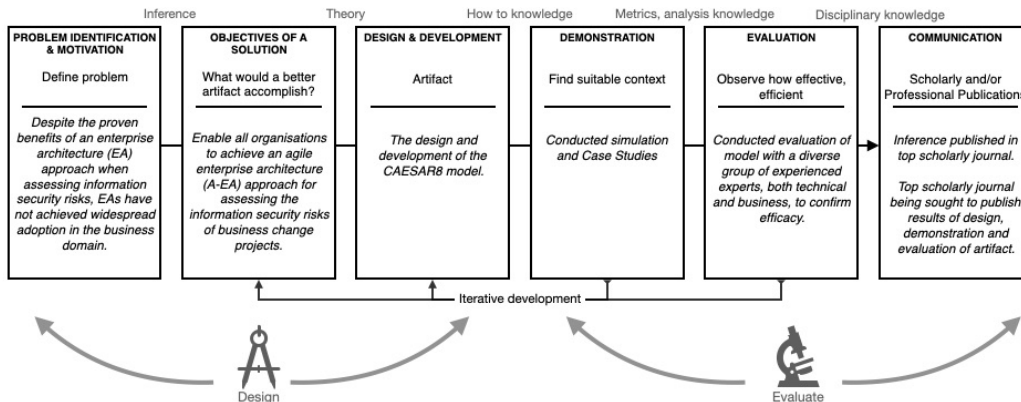


Figure 3.1: Using the DRSP model for the CAESAR8 artifact design

Following the DSRP model ensures that I have followed a consistent DSR research process that provides the necessary rigor in my research. It ensures that problem identification in the target domain is properly formulated and controls the selection of my design objectives¹. This rigor is then reflected in the DSR output, ensuring that each iteration of the artifact has been demonstrated to provide a traceable design benefit², and culminates in an ex post evaluation of the finished artifact.

All 6 steps of the DSRP model were followed in the design of CAESAR8. Steps 2-4 were repeated over five successive iterations of the artifact³. This is typical of the DSR approach to research, where artifacts are developed by completing a series of design and evaluation cycles [95]. Initial versions of CAESAR8 were conceptual models - Artifact Conception Versions (ACV), to enable the concept to be shared and discussed with other researchers and business representatives. Later versions of the model were Artifact Prototype Versions (APV).

Even though a full commercial version of the CAESAR8 model was beyond the scope of this study, the APV versions allow more in-depth testing of the concepts, with the final version being a multi-user working prototype of the

¹Table 4.3 shows how Design Goals have been matched to Problems.

²Table 6.2 shows how Design Goals have been addressed by artifact design iterations.

³Table 6.1 summarizes how iterations of the model were designed and evaluated.

model to support an *ex post* evaluation of the design that allowed business professionals to conduct trials of the model.

3.2 Design Science Research Process Overview

The design process is covered by the first 3 steps and the evaluation is covered by the last 3 steps. This process is not linear but is a cyclical process, and this ensures that each artifact iteration is tested against the design objectives and improved for the next iteration. Designing the artifact required a frequent transition between the design and evaluation steps, so that the design was able to mature and achieve the maximum perceptible benefit.

The first step in the DSRP model is to determine the problem that needs solving: **Problem Identification and Motivation**. This step is a summary of my earlier systematic literature review and analysis that was described in Chapter 2.

For my evaluation under Design Science Research (DSR), I have used a “design-evaluate-construct-evaluate” pattern [177]. In other words, the design of the artifact is evaluated before and after construction. Ex ante evaluation was carried out by conducting *demonstrations* using early internal testing and case studies. The final, ex post evaluation was carried out by experienced industry experts, and was completed after the fifth and final iteration, and therefore final construction, of the CAESAR8 model.

Each evaluation cycle has informed the design. For DSR to be successful, it requires a good knowledge of the business domain. As researcher and designer of CAESAR8, I am an experienced information security professional. My experience of working in the business domain for 37 years has meant that I am able to contribute to a real-life evaluation of the artifact, and I conducted early case studies of the CAESAR8 model. However, I did not take part in the final ex post evaluation.

Figure 3.2 provides a 3D representation of how the successive iterations

take the design process from the initial identification of the problems through to a completed artifact in the form of the CAESAR8 model. The numbers against the boxes represent the models design iterations.

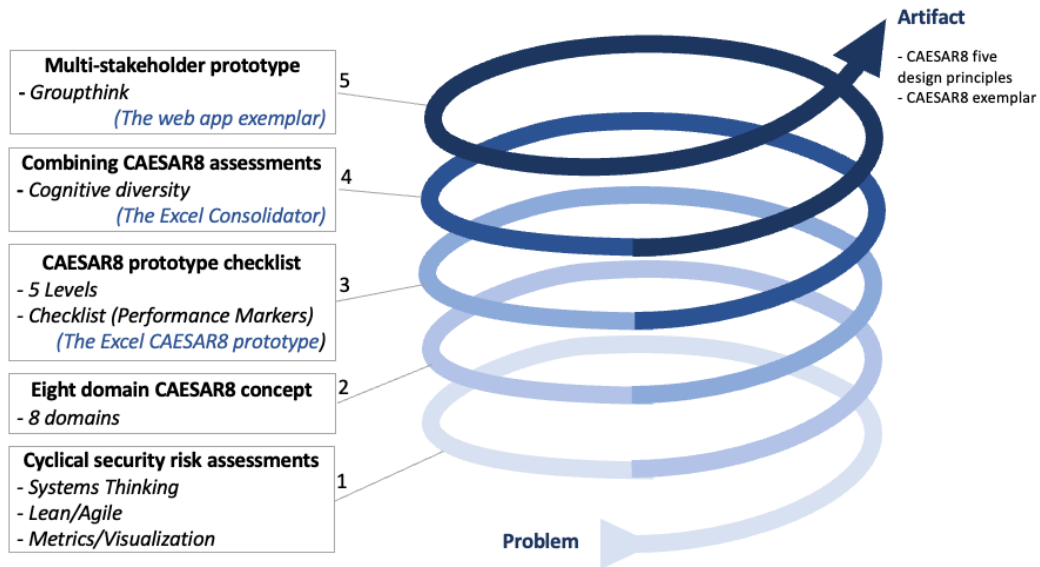


Figure 3.2: Evolution of CAESAR8 model over 5 iterations, resulting in the 5 CAESAR8 design principles for holistic ISRM and a CAESAR8 exemplar

The first iteration defined the structure of the artifact, and was heavily influenced by my research on agile values and the visualization of metrics. Then came the identification of the eight domains, followed by the five levels that form a standardized checklist and provide a common frame of reference for assessment. The checklist is significant as it also allows stakeholders from non-security backgrounds to conduct consistent, meaningful and repeatable assessments in the CAESAR8 model. Finally, human behavioral-science characteristics have been incorporated into the design. Empirical studies into behavioral science have shown the value of obtaining diverse, independent stakeholder assessments, and how these need to avoid *groupthink* scenarios. Following a formal evaluation of the model by industry experts, some improvements to CAESAR8 were identified.

Each of the DSRP steps is summarized below and they are described in full within their respective chapters in this thesis.

3.2.1 Step 1: Problem Identification

My hypothesis was that many organizations value the potential benefits of EA but are unable to implement a practical EA in their environment. Theories for this include the drain that it imposes on resources; that it creates a potential delay on projects, as artifacts are created, reviewed and maintained; and it seems contrary to concepts of lean and agile, which so many organizations aspire to. Where EAs are used, they are often fragmented and/or inaccurate and there is little evidence that they actually deliver the overall benefits to the enterprise that is proclaimed.

After completing my systematic literature review in Chapter 2, I concluded that a new approach to achieving the benefits of an EA was urgently required.

3.2.2 Step 2: Objective of the Artifact

The main purpose of my study was to improve the use of EA concepts for the benefit of ISRM in business change projects. Therefore, my objective was to design a practical artifact that optimizes ISRM in agile projects. The artifact does not require specialist resources, does not focus on unnecessary EA artifacts and fully supports agile values.

The detailed objectives were created by referring back to the systematic literature review and extracting the Problem Identification references. The Underlying Causes were also also significant for the design as I needed to make sure that my objectives would overcome the common constraints encountered in business. The additional Information items also needed to be considered.

These detailed objectives for the artifact have been defined as the Design Goals, and they are described in Section 4.2 - "Objectives of the Artifact". The design goals are summarized in Table 4.3, which details how the goals were designed to address the original problems described in Chapter 4.

3.2.3 Step 3: Design and Development

The design and development process (DSRP Step 3) involved conducting root cause analysis into ISM failures that are documented in scientific literature. The rigorous DSR process has demonstrated the performance of the artifact's design over five iterations, which included further search of the literature so that I could incorporate areas of human behavioral-science.

My approach to designing and developing CAESAR8 was to produce a novel scientific model that could be developed into a commercial product at a later stage. However, for testing the efficacy of the model, I have created three IT instantiations of the CAESAR8 model to help the design, development and evaluation processes. The first two used Microsoft Excel and the last instantiation was a multi-user web app based in the Cloud and was used by professional volunteers for an external evaluation process (DSRP Step 5).

3.2.4 Step 4: Demonstration

The **Demonstration** step (DSRP Step 4) was undertaken as part of the iterative design and development process to demonstrate the performance of the model and direct further design and development to mature the artifact. The case studies were selected on the following basis:

Iterations 1 and 2 provided static demonstrations of the artifact's style. This was shared with other researchers and cyber security experts.

Iteration 3 used a case study that was selected to test if the performance makers uncovered the issues described in an investigation of the case. This iteration also included another case study using a synthetic scenario created by the author. The purpose of this study was to check the consistency of CAESAR8 results and, therefore, the objectivity of the performance markers, by observing if two different assessors who possess similar knowledge are likely to provide the same result. To support both of these demonstrations, an MS Excel spreadsheet instantiation of the model was created.

Iteration 4 tested the artifact's ability to combine multiple perspectives into a single assessment to uncover otherwise hidden ISRM problems. It also served a secondary purpose to test the artifact's ability to be applied in

operational technology scenarios. For iteration 4, an MS Excel Consolidator spreadsheet was also created that automatically combines multiple MS Excel assessments into a single result. Various rules for the consolidation process are described.

Iteration 5 repeated the case study for iteration 3 but using the latest design that allowed for the different perspectives of stakeholders to be selectively taken into consideration. This iteration used a new web app that was created for the ex post evaluation.

All but one of case studies were based on real-life scenarios that had been well documented in the public domain. The other case study was based on a synthetic scenario created by the author for the purpose of examining the consistency of responses. This synthetic scenario deliberately lacked direct references to the performance markers, so that the assessors interpretation of the scenario, and their subsequent response to the performance markers, could be examined⁴.

3.2.5 Step 5: Evaluation

The Evaluation process is an essential part of Design Science Research [72]. Hevner et al. describe how a design artifact must be rigorously demonstrated via well-executed evaluation methods. A specific evaluation framework is described by Pries-Heje et al. [137]. This framework describes how the evaluation process should operate in two dimensions throughout the design of the artifact. The first dimension describes whether the evaluation is based on forecasts of early iterations (*ex ante*) or actual results of the final design (*ex post*). The second dimension describes whether the evaluation is naturalistic or artificial.

Ex ante demonstration exercises were performed during the early design of the artifact and were described in Step 3 above. The formal ex post evaluation of the artifact for Step 5 of the DSRP process was conducted after

⁴In a real business scenario, those who have ISRM responsibilities would not usually have first-hand knowledge of the situation that they are assessing.

iteration 5.

In respect of the second dimension, my evaluation is classified as an *artificial* evaluation since it is based on case studies or tests conducted by independent business professionals.

All IT solutions described in the thesis have been created specifically for the demonstration and evaluation of the artifact. These instantiations do not constitute design iterations in themselves, and will not be used for any other purpose. The artifact that I describe in the thesis is only the abstract CAESAR8 model that is based on the CAESAR8 design principles. The working IT instantiations are essential for a rigorous evaluation of the model, but are not the focus of the evaluation. Hence, all design up to and including the development of the Excel instantiation in Iteration 3 and the Excel Consolidator in Iteration 4 are *ex ante*. Evaluation after this involving the cloud-based web app, include all major characteristics for the final design and are therefore considered *ex post*, see Figure 3.3.

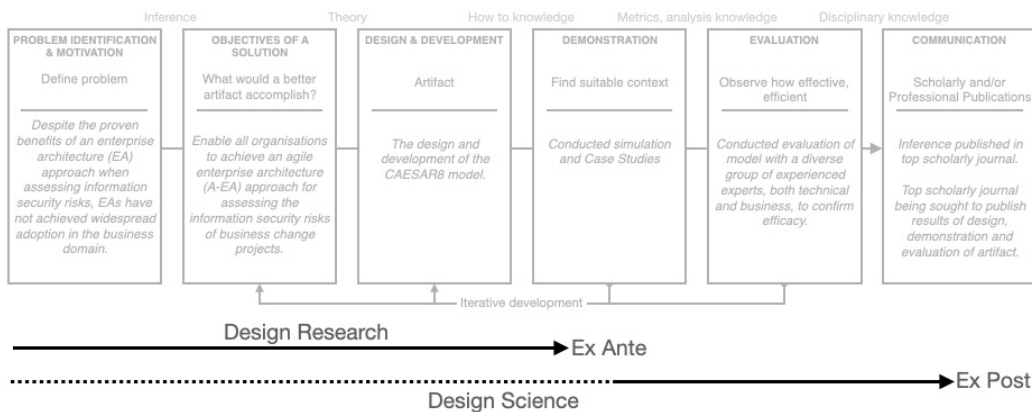


Figure 3.3: Evaluation Strategy

To use the evaluation framework as a tool to improve understanding of the evaluation strategies, Pries-Heje et al. [137] pose three questions that are required to be answered: (1) *what* is actually being evaluated; (2) *how* is it being evaluated (what process, and against what criteria); and (3) *when* is it being evaluated? These questions provide the process (P) and criteria (C)

for the evaluation. For the evaluation of my artifact, the following answers to these questions are:

What: An IT solution needed to be created for the Process (P) described below, so that CAESAR8 can be experienced to work and tested reliably. However, to develop a fully working artifact that could be tested in a real-world scenario would require a substantial amount of development time and is both not achievable for the thesis, and is beyond the scope of this DSR. An IT instantiation was designed to support the evaluation work, but no more than this.

How: This process complies with the *Dynamic Analysis* method of design evaluation that is described by Hevner et al.[72], where the artifact is studied in use for dynamic qualities, such as the performance specified by the design criteria. By evaluating the artifact against multiple criteria in this way, it also helped remove confirmation bias⁵, as participants in the evaluation were rating very specific features of the artifact after testing the artifact's performance using project scenarios with which they are personally familiar.

The evaluation included: i) a pre-evaluation questionnaire to evaluate the accuracy of the problem identification; ii) hands-on testing of the fully-working artifact; and, iii) a post-evaluation questionnaire to evaluate how well the artifact met its design objectives.

The Process (P) needed to provide the necessary rigor and so the evaluation was conducted by independent experts who individually have more than 10 years experience of working on information security related projects. The artifact is designed to bring together diverse experiences across key disciplines, therefore, the experts needed to have diverse backgrounds to provide greater accuracy in the evaluation, for example: Information Security Professionals, Auditors, Software Engineers, Project Managers and Business Risk

⁵A tendency to favor prior held beliefs.

Managers.

The Criteria (C) for the evaluation was purposely unbounded so that experts could evaluate the artifact using their own projects, scenarios and experiences. A platform for the ex post evaluation was provided in the form of an IT instantiation of the artifact. This was a cloud-based web application developed for the purpose. This web app provided experts with the ability to create multiple assessments and then view the consolidated results. Experts were permitted to selected different values for performance markers and then consolidate these in different ways by selecting which assessments to consolidate.

Specifying fixed criteria would have limited the value of the evaluation exercise and would not have yielded meaningful results, since the experts were always expected to have differences of opinion on the assessments. Their response to their own evaluation was the most important aspect.

The twelve Design Goals were individually assessed by the experts post-evaluation to determine how well they have been met by the artifact.

In addition, to confirm that the artifact is providing real benefits to the problems identified (DSRP Steps 1 and 2), the fifteen common problem areas (see Section 4.1.1) that were reviewed by the experts at the commencement of the evaluation, were revisited post-evaluation to confirm the artifact's contribution.

I was also able to verify how the web app had been used by inspecting the data that experts had created during the evaluation.

When: The final artifact needed to be evaluated rigorously by users and security professionals who have good business experience, since the artifact is designed to benefit real organizations. It was therefore *ex post*, i.e., based on the tested performance of the finished artifact rather than forecasts.

In conclusion, based on the Pries-Heje et al. framework [137], my formal strategy for the final evaluation process for the artifact is shown in Figure 3.4.

	Ex Ante	Ex Post
Naturalistic	Process / Criteria	Process / Criteria
Artificial	Process / Criteria	P: Experts test a simple web app of the model and respond to pre and post questionnaires about the artifact's design. C: Experts use own scenarios to test, plus respond to research problem areas and design goals.

Figure 3.4: Evaluation Strategy for CAESAR8

3.2.6 Step 6: Communication

My artifact's design incorporates five novel design principles that are relevant to theoretical research of enterprise architectural concepts for ISRM, and these need to be shared with the academic community. My literature review and analysis has already been published and cited in a quality peer-reviewed journal:

Loft, P., He, Y., Janicke, H. and Wagner, I., 2019. Dying of a hundred good symptoms: why good security can still fail-a literature review and analysis. Enterprise Information Systems, pp.1-26.

This paper described the study conducted for my first research question (RQ1) and included details of the eight domains. It also included my research on the influence that individual factors have on other factors of information security management (ISM).

I am also in the process of submitting a second paper that describes the results of my second research question (RQ2), which is the final design of the CAESAR8 model and the results of the independent evaluation process.

This second paper explains the significance of the CAESAR8 five design principles and includes details of the evaluation of the CAESAR8 exemplar. The CAESAR8 exemplar model is also valuable to the business community as it provides a practical foundation for a working artifact, see Section 1.6.

3.3 Conclusion of Research Methodology

In this chapter I have described how I have used the Design Science Research (DSR) methodology to develop the CAESAR8 model. Following a DSR approach has enabled me to blend human behavioral-science with design-science research in a manner that also incorporates my own empirical knowledge of the subject domain.

I have described the specific DSR process that I followed, starting with a systematic process to define the problem and objectives of my artifact. Continuing the DSR process led to five design and development iterations to finalize the CAESAR8 model. I progressed the design of the model from early Artifact Concept Versions (ACVs) to Artifact Prototype Versions (APVs) that could be demonstrated by case studies and finally, an ex post evaluation conducted by industry experts. Conducting early ex ante demonstrations of the APVs identified where I needed to make improvements to the design of the artifact. This helped to ensure that the final iteration was optimized before the external ex post evaluation.

The DSR process included a final step (DSRP Step 6) to communicate my research. My literature review and analysis has been published to the academic community and I will publish a summary of the final CAESAR8 model design principles for the benefit of further academic research.

As the final design is a practical model for industry, I will also communicate the concept to more business-focused journals and conferences.

A case study that I used to demonstrate the CAESAR8 model was the risk analysis of an operational technology (OT) perspective, the Boeing 737MAX. The CAESAR8 checklist can be applied in a safety context and can blend security and safety risk analysis to provide a security informed safety context. I will communicate this specific benefit of the model's design.

Further, I will publish details of the methodology that I devised to conduct my systematic literature review and analysis, as this proved to provide an accurate and reliable assessment of the most relevant scientific research.

Chapter 4

Problem identification and objectives

The primary objective of the CAESAR8 model is to address that the original problem areas identified in the literature review (Problem Identification, from DSRP Step 1). The design goals for CAESAR8 (Objective of the artifact, from DSRP Step 2) were then determined from problems identified.

4.1 Problem identification

Having completed my systematic literature review and analysis I read multiple calls for research to address problems associated with an accurate assessment of information security risks in agile projects to ensure that they remain aligned with business changes.

Details of these findings were provided in Section 2.2.2, where I labeled these problems as *Problem identification* and *Underlying issues*, and they are summarized in the next two sections.

4.1.1 Fifteen common business problem areas for information security management

During my systematic literature review, I identified where specific problems exist for ISRM within a typical business environment and these will hinder the effectiveness of any EA implementation. Fifteen common problem areas are observed and they are labeled *Problem identification* in the text. I summarize these below and classify them as either governance or design issues:

- Governance Problems
 1. Stakeholders not directly engaging with projects
 2. Lack of collaboration across separate teams
 3. Limited understanding of the wider effects of changes
 4. Executive not formally understanding project risks
- Solution Design Problems
 5. Legal compliance reviews not completed for all changes
 6. Security risk management not expressed in a business context
 7. Insufficient rigor applied when working with third parties
 8. Agreed security controls are sometimes omitted
 9. Lack of monitoring of security controls
 10. Project impact on current business processes not fully considered
 11. Lack of clarity over information storage and sharing
 12. Ad hoc deployment of new technology
 13. Not understanding the effect of a new system on all personnel
 14. Testing is not completed adequately
 15. Management unwilling or unable to monitor compliance

Whilst some of the problems identified could be resolved by providing good documentation (for example, item 14 requires test plans and item 7 requires quality third-party contracts), this was not true of all of the problems.

Item 1 refers to stakeholder engagement, which is difficult to enforce even with quality EA artifacts, and item 9 requires monitoring.

An intentional benefit of the CAESAR8 model is supporting non-EA environments so that they can benefit from EA approaches to ISRM. Therefore, addressing these problems is an important requirement for the design of CAESAR8 and not necessarily on supporting the implementation a commercial EA framework. A more significant benefit for the CAESAR8 model is supporting the EA process in an agile and repeatable manner, rather than pursuing the perfectly documented EA artifact.

The evaluation phase of my DSR process needed to test these 15 problem areas with other experienced professionals to determine how widespread these problems are.

4.1.2 Underlying issues for security strategies

The *Underlying issues* affect the reliability of ISRM process but are issues that CAESAR8 can not change. As is the case with the 15 problem areas, these issues also need to be confirmed later with other experts. The issues are summarized as:

Underlying issues for security:

1. Time-related pressures are a risk to security
2. Budget constraints are a risk to security
3. High workloads are a risk to security
4. Volume of project changes are a risk to security
5. Difficult to recruit skilled security personnel
6. Prioritization of work can be unclear
7. Disparate security and business risk management methods
8. Security documentation sometimes inadequate
9. Lack of adherence to security operating procedures

4.2 Objectives

The main design objective for the solution was derived from the Problem Identification (DSRP Step 1) and summarized in Section 4.1 above. In addition, since the CAESAR8 model needed to comply with agile/lean concepts, I included lean principles in the objectives for CAESAR8.

In summary, these sources for the CAESAR8 model's objectives were:

- The 15 common problem areas identified - Sub Section 4.1.1
- The 6 guiding Lean principles - Sub Section 2.3.3.1
- Plus, the 9 underlying issues for businesses - Sub Section 4.1.2

4.2.1 Addressing known problems and underlying issues

The benefits of EA need to be achieved without recourse to the creation of complex top-down EA artifacts. My CAESAR model enables organizations to build-out the architecture in a more agile way. In this way, an organization's EA will become more adaptive to the needs of the business.

My objective was to design a novel model that provides an agile, holistic review of projects as they progress so as to capture any change in key information security risk factors. The CAESAR8 model should only encourage the timely production of EA artifacts that benefit the immediate project under review, and not be sidetracked by compliance with the detached characteristics of international security standards.

My research delivers an improvement in the form of a “new solution to a known problem” [173], since CAESAR8 is not a new EA framework and, to the best of my knowledge, a model that addresses the problems of EA in this way does not already exist. The remainder of this chapter will describe how the goals have been derived from the Problem Identification (DSRP Step 1) and have incorporated agile values and lean principles.

4.2.2 Agile and Lean

For the CAESAR8 model to be able to address its design objectives, lean and agile concepts are always a key requirement of my research proposal and my review of the literature identified that this should be a key goal for CAESAR8. I had already determined that only the overarching agile values were important to the design. Snee's guiding principles for lean [161] are built into my design of CAESAR8 and will be applied in a way that also covers the agile values. These lean principles can be matched to agile values:

Lean principle	Agile value
Have a sense of urgency	Working software over comprehensive documentation
Review regularly	Responding to change over following a plan
Understand human behavior	Individuals and interactions over processes and tools
Make it easy	Customer collaboration over contract negotiation
Always have an impact focus	
Use improvement as a leadership development tool	

Table 4.1: Lean and Agile design requirements

4.2.3 Additional design information

In addition to the primary design goals to meet the design objective, I ensured that all of the additional design considerations that I noted from the systematic literature review were taken into account. These were identified as the *Information* category. Table 4.2 summarizes these points and describes how the design of the CAESAR8 will capture them.

Additional Design Consideration	Design Approach
CAESAR8 should support the future proofing of a change by supporting state-of-the-art design	Do not restrict solution design and include as a separate optimization level to encourage this
Always encourage the development of a strong security culture	Addressing the 15 problem areas across departments should help to build a strong security culture
Guard against working with out-of-date EA artifacts	CAESAR8 must capture tacit knowledge in real-time and not make EA artifacts the central goal
Ensure EA maintenance is not a costly process	Ensure quality documentation is not the key focus. Keep the checklist easy to understand
Support early prototyping of solutions and continuous reviews thereafter	Share knowledge of the solution and include testing of iterations in the design
Involve business stakeholders in information security risk estimations	Review all changes with relevant parts of the business to determine actual security risk
International standards are valuable reference baselines but do not align to actual business risk	CAESAR8 must not use international standards as a holistic checklist

Table 4.2: Additional design considerations

These points do not require testing in the evaluation step as they were general observations that are related to a pre-existing experience of EA and are intrinsic to the design of the CAESAR8 model. Although they were not a fundamental part of the root cause analysis, they are nevertheless design features that were observed and taken into consideration in the design of the model.

4.2.4 Design Goals for CAESAR8

The problems described in Section 4.1 and the additional design requirements described in this section were analyzed and twelve design goals were created for CAESAR8.

Below is a description of the final design goals.

1. **Base the artifact on a non-linear design that supports and encourages continual reassessments of ongoing changes to projects.**
The artifact must ensure that the full assessment is able to be repeated whenever new information is known about a project. This is to identify new risks and confirm the results of mitigating actions.
2. **Progression through the artifact should reflect the dependency between security activities.**
The sequence of security activities is important, and the metrics for progress must be clear to all users. The levels built into the artifact must represent levels of maturity based on these sequences.
3. **It must be possible to integrate the artifact within existing project processes.**
The artifact must be agnostic to development and project methodologies, allowing for its integration into any environment. It must also support standalone use (particularly for smaller organizations).
4. **The artifact must support integration with agile working practices.**
The artifact must fully embrace the core values of agile working while remaining agnostic to specific agile working methodologies. It must support the concept of continuous reviews of project changes and new development iterations.
5. **The artifact should support the creation of architecture documentation, where required.**
The artifact should provide input to the maintenance of any existing EA documentation, with a preference for just-in-time documentation. This preserves the concept of building out the architecture in real-time.
6. **The artifact must focus on the key issues that determine the success of information security in business change projects.**
To achieve this in reality, the artifact must present a tractable checklist

of these issues that provide an holistic review of information security risks for business changes.

7. The checklist must be clear and easy for all stakeholders to understand.

This is a critical requirement, given the intention to use the artifact with a diverse group of stakeholders (IT and non-IT).

8. It must be an easy process to conduct assessments using the artifact.

Particularly given the infrequency of conducting assessments for some stakeholders, it is important that the artifact is not difficult to understand and use.

9. Conducting assessments must be a quick process.

The artifact is likely to be used as an additional control step to help keep project security activities aligned. It must therefore be an expeditious process.

10. The artifact must assist with the prioritization of work.

Progress will not be reliable if underlying issues go unaddressed or are undertaken in the wrong order. All stakeholder assessments must be preserved, to allow for a constant reassessment of progress in relation to their identified issues. Focus must be prevented from shifting to one particular issue but must be a constant reassessment of the whole to identify true progress and priorities.

11. Assessments from stakeholders across the organization have to be combined to ensure that information security solutions are correctly aligned with the business.

Stakeholders must be free to examine the effect of business changes in their own particular context, and allowed to conduct their assessments separately, thus avoiding the issues associated with groupthink. The assessments are aggregated in a way that preserves all stakeholders' original judgments and opinions.

12. It must be easy to share the overall results of assessments with colleagues and management.

Sharing of results will take place at all levels of the organization, so the status of assessments must be immediately clear to any audience. The artifact must present clear and concise metrics in a format that does not require understanding of complex technical architectures or information security standards, allowing the joint reviews of all key stakeholders.

4.2.5 How the design goals address the identified problems

The Design Goals are summarized in Table 4.3, with a cross-reference to the problem areas, underlying issues and lean principles. They have been arranged into logical groupings for design, usability and governance, to aid the design of the CAESAR8 model.

#	Essential Design Goals	15 Common Problems	Lean Principles	Underlying Issues
Design focus				
1	Base on a non-linear design that encourages continuous re-assessment of changes	10	2, 3	6
2	Progression must reflect dependencies between deliverables	5, 7, 8, 9, 11,12, 14, 15		8, 9
3	Allow integration into project management processes or operate stand-alone		1, 2	4, 6
4	Fully embrace Agile values		(all)	(1-4 cause)
5	Encourage just-in-time updating of EA artifacts		1, 2	1
6	Focus on the key issues that prevent common IS failures	(all)		9
Usability focus				
7	Provides an easy to understand, repeatable review of the most critical issues		2	1, 2, 3, 4
8	Easy to complete assessments		4	5
9	Quick to conduct assessments		1, 2	1, 3
Governance Focus				
10	Help to prioritize project work		1, 5	6
11	Ensure all business departments' perspectives are represented	1, 2, 3, 6, 10, 13	3	7
12	Easy to interpret and share results at all management levels	4, 6, 10	3, 6	7

Table 4.3: The essential design goals address the problems identified

Table 4.3 shows clearly that, whilst the problem identification areas are an integral part of the design, and the analysis of coding of the literature was key to creating the 40 performance markers in CAESAR8 (item 6), they only constitute a third of the design goals. The underlying issues were key to

identifying all design goals for the CAESAR8. Also, including lean principles helped to refine two thirds of the overall design goals.

By including all of these problem sources when defining the design goals, the CAESAR8 model has been able to meet its overall design objective.

4.3 Conclusion of Problem Identification and Objectives

This chapter summarized the problem areas and underlying issues that were identified from the literature review that I described in Section 2.2.2.

In addition, my study of Lean and Agile, identified that Lean principles and Agile values were highly relevant to the CAESAR8 design but that it would not be beneficial to tie the model to specific methodologies. Focusing on the overarching concepts allowed me to design a solution that could be used by all project stakeholders, regardless of project management experience, and in a way that remained agnostic and could be used standalone.

Design goals were established for the CAESAR8 model that addressed the problem areas. When creating the design goals, I also considered the underlying issues and Lean principles that I obtained from the literature. This was an important consideration, as over half of the design goals for the CAESAR8 model were created from these two additional factors.

Chapter 5

Root cause analysis of IS performance to inform CAESAR8 design

During my systematic literature review to identify **problems** in ISRM, I had coded the literature. I now wanted to analyze the coding to uncover the root cause of information security problems.

In this chapter, I use the mixed methods of quantitative and qualitative analysis to synthesize the information for use in the design of CAESAR8. This work helped to answer my second research question (RQ2), which is to find an **Agile solution**. Whilst the Problem Identification step had identified *what* problems CAESAR8 needed to help resolve, this analysis provided information as to *how* they needed to be resolved.

This Chapter forms part of DSRP Step 3, design and development.

5.1 Quantitative analysis of the coding

This quantitative analysis was conducted to help determine the root causes of IS project failures, so that I could focus the design of my artifact in these particular areas.

To identify how the nodes that I created during the systematic literature re-

view influenced the success of other nodes, I conducted pairwise correlation of the nodes. To do this I constructed a large pairwise correlation matrix that contained 4,225 cells (65 nodes \times 65 nodes), and this is shown in Figure 5.1. In addition to the 65 *root cause* nodes, I also included each node's correla-



Figure 5.1: Pairwise correlation matrix for all 65 nodes

tion with the *effect* nodes (*success* or *failure*) and the *sector* nodes (*public* or *private*).

A detailed examination of strong pairwise relationships helped determine how factors are related and how specific information security management actions have an effect on the success of other nodes. I decided to examine these influences in greater detail, so that I could identify what factors are the most important to include in the design of CAESAR8.

I determined the *influence* of each node by calculating the mathematical product of its correlation to the success or failure nodes (whichever is greater) and the number of other nodes that it has a significant correlation with. The influence value corresponds to the area that each node delineates in the scatter chart shown in Figure 5.2 when drawing a rectangle from the graph origin.

Since correlations where $r < 0.3$ are considered to have little correlation, I only counted nodes with $r \geq 0.3$ ¹. The influence for each node i as follows, with j denoting the nodes except i :

$$\text{influence}_i = \max(r_{i,\text{success}}; r_{i,\text{failure}}) \times |j|, \text{ where } r \geq 0.3$$

¹The highest actual node count for $r \geq 0.3$ was 34 nodes.

The resulting influence values are between 0 and 20, with 20 being the most influential (i is in [0.3,1] and j is in [1,65]). $r_{i,success}$ is the highest correlation to the *success* node and $r_{i,failure}$ is the highest correlation to the *failure* node.

Figure 5.2 shows the nodes in an X-Y scatter chart. Nodes are positioned in relation to their overall effect on success or failure and their correlation with other nodes, although the exact details of those relationships are not significant at this stage in my analysis.

The figure is divided into quadrants. The nodes in the bottom-right quad-

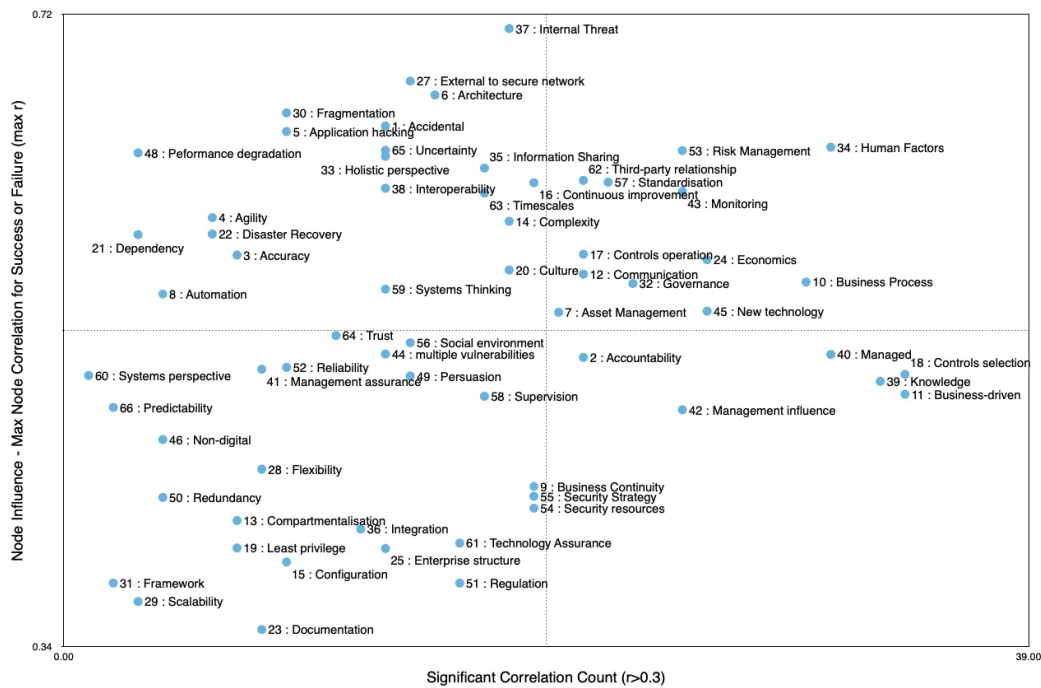


Figure 5.2: Node Scatter Diagram (success or failure versus pairwise correlation)

rant have a significant correlation with many other nodes, but only a weak correlation with success or failure. This often means that, while they are not one of the highest contributors to success or failure, they are a significant contributor to the success or failure of other nodes; for example *Business-driven*, or *Knowledge*. For the top-left quadrant, the reverse is true, where

nodes have a strong influence on success/failure but little correlation with other nodes. The nodes in the upper right quadrant show both a high correlation to IT Security performance, and a high correlation with other nodes, with Human Factors being the most influential. The graph shows that the effect that each node can have on the success or failure of a project, or on other nodes, can be quite diverse and requires more detailed analysis.

To advance the optimum design for my artifact, I conducted further analysis of my coding to identify the themes that were present in the data. This work is described in the next section.

5.2 Qualitative analysis for node domains

Whilst I had documented my original findings of the literature review following the 6Ws categorization, see Section 2.2.2, the 6Ws classification was not providing the best fit for the information that I obtained from my review and analysis. The 6W classification of information did not emerge from the literature and it would be confusing to try and fit this information to the 6Ws framework. Consequently, it was not going to make the best framework for CAESAR8.

Some key themes were identifiable from the data in relation to how the nodes fall into different themes. For example, *human factors* appeared many times in the literature, but it was associated with many different nodes. Whilst individual behavior has a significant impact on information security risks, there are also different considerations for how people operate in groups, or how individuals that have management responsibility can impact the security culture.

Therefore, I conducted qualitative analysis of my coding by following inductive (bottom up) thematic analysis [27]. By referring back to the source references for each node, this method ensured that my analysis remained impartial and was based on the data that I had collected from the articles. When determining the themes, my analysis focused on the most influential

nodes, that is nodes that have a strong influence on success or failure and/or those nodes which have a strong pairing with other nodes. These are the nodes that appear in, or near to, the upper-right quadrant in Figure 5.2.

For this analysis, I selected nodes that have an influence value ≥ 8.0 , because that was the median of all node influence values. Statistically, the median is the most likely influence value for a given node, and is less likely to be affected by abnormally high or low values.

As a result of focusing on the high influence nodes, I identified eight themes and I called the themes *domains*. I then checked all of the 65 nodes, and found that I could place all of them into one of these domains.

The domains are: Business Process (BP); Enterprise Architecture (EA); External Factors (EF); Human Factors (HF); Information Assets (IA); Management Influence (MI); Security Governance (SG); and Technology Infrastructure (TI). A summary of the domains is shown in Figure 5.3.

External Factors (EF) captures external factors that influence the effectiveness of security strategies, such as economics and third-party relationships. Security Governance (SG) ensures that security-related decisions fulfill the needs of the business, including time-related pressures. Business Process (BP) assesses the security impact on current business processes, and the preparedness for business change. Information Assets (IA) reviews the ongoing management of information assets, particularly those that cross traditional corporate network boundaries. Technology Infrastructure (TI) provides a review of how technology is being implemented within the organization to ensure that it meets the requirements for information security. Human Factors (HF) monitors the human impact of a business change to increase the likelihood of success. Management Influence (MI) reflects the significance of middle management engagement for ensuring that security requirements continue to be met. Enterprise Architecture (EA) ensures that a business-driven strategy is aligned with the programs of individual business units and, where necessary, EA artifacts are created and updated to support the change.

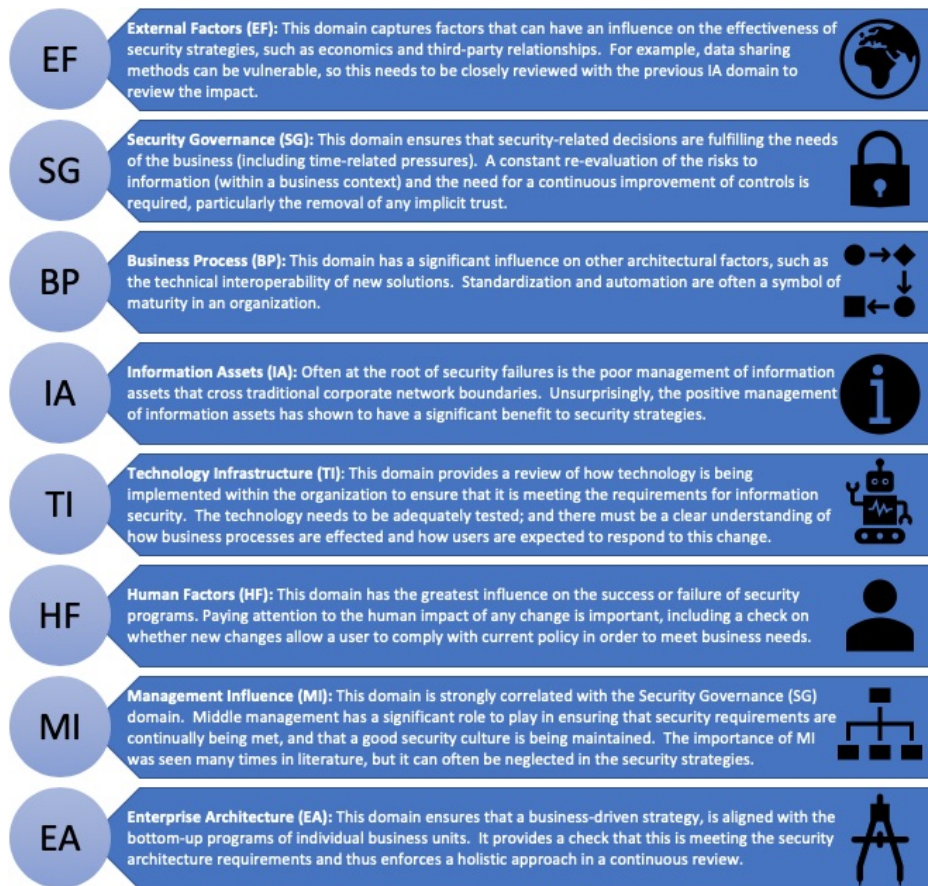


Figure 5.3: Summary of the CAESAR8 domains and what they represent

A table showing all of the nodes and their respective domains is provided in Appendix A. This table also includes the results of the quantitative analysis conducted in the previous section that helped to focus the thematic analysis on the most influential nodes.

Figure 5.4 shows the relationships between the domains in a cobweb diagram to aid further analysis. The correlation values have been determined by examining each high-influence node for each domain (influence ≥ 8.0); selecting all of the nodes that this high-influence node has a high pairwise correlation with ($r \geq 0.5$); and, then determining which domain the paired correlation relates to. This method ensures that nodes that have a strong correlation to nodes with a high-influence factor are all considered in my

analysis.

The thickness of the links represent the maximum strength of the correlation values. For example, *Security Governance* is strongly dependent on *Management Influence*, and *Technology Infrastructure* has to be aligned with *Business Processes*. Further analysis identifies what the key factors are that help determine the most successful IS performance.

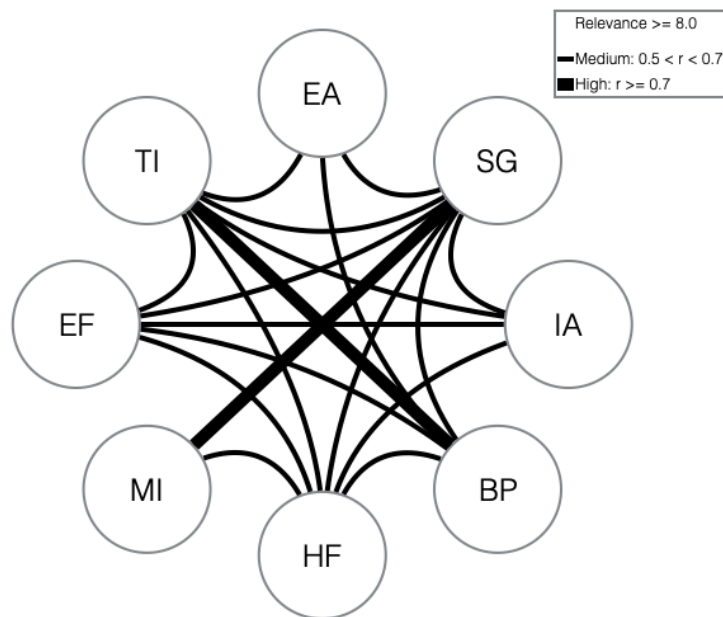


Figure 5.4: Cobweb Diagram: shows strongest correlation between domains

Figure 5.5 shows how the eight domains are distributed across the node scatter chart. A blue line (with blue label) is shown in Figure 5.5 and it represents an influence value of 8.0. Those nodes with an influence value of >8.0 are situated above and to the right of this line. All the domains feature well inside the top-right, high-influence area of the scatter chart and this provides confirmation on the relevance of the eight domains in addressing those issues that have the most influence on ISRM.

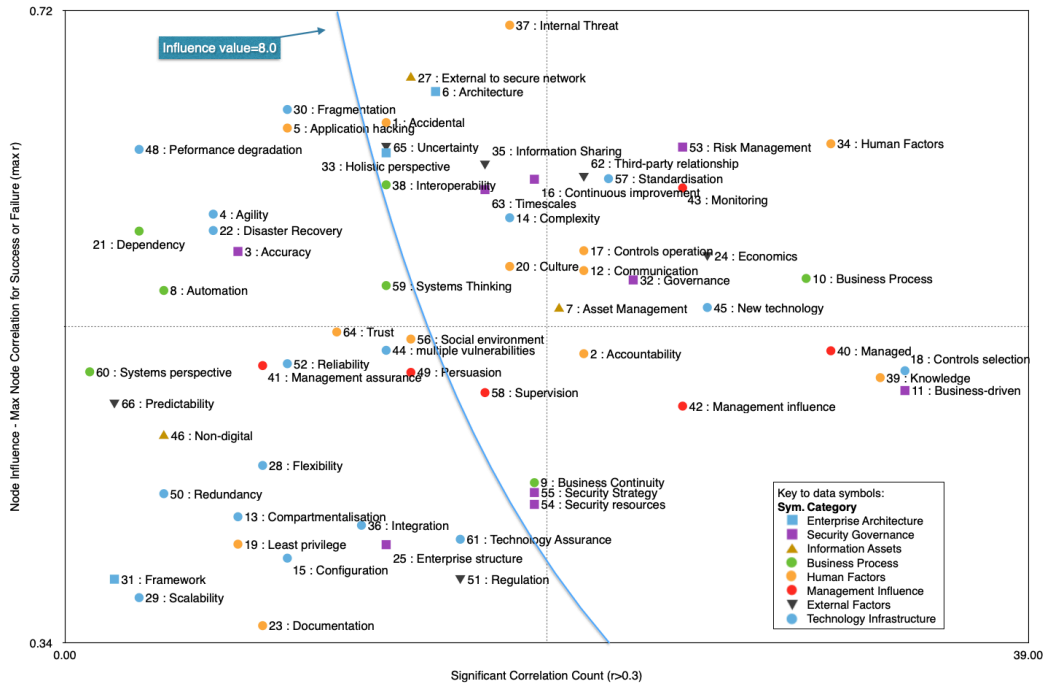


Figure 5.5: Node scatter diagram showing coverage of the domains and the high-influence boundary

A description of the eight domains for holistic ISRM is provided in the next eight sections. Only nodes that have a influence value ≥ 8.0 are included in the description.

5.2.1 Information Assets

Table 5.1 lists the high-influence nodes that are in the IA domain. The **External to secure network** node (with $r=0.68$) relates to the poor management of assets leaving the secure network [2, 31]. This node has a strong correlation with the EF domain for its **Information sharing** node ($r=0.69$). These findings are described further in the next section.

Category	Node	Node Influence
Information Assets	Asset Management	9.51
	External to secure network	9.51

Table 5.1: Information Assets Domain

The strongest correlation to the SG domain is with **risk management** ($r = 0.63$). This is the highest success correlation for risk management and it is with the **Asset Management** node. An architecture should determine what assets are important to an organization and their true value [63]. This is often achieved by considering the sensitivity of data before conducting risk assessments [26]. This ensures that the cost-benefits of security solutions can be evaluated before procurement and implementation, and that only the necessary level of security is applied.

5.2.2 External Factors

As shown in Table 5.2, there are several external factors (i.e., EF nodes) that greatly influence the success or failure of information security, and the **Economics** node is the most significant external factor ($r = 0.57$, and it is for failure references). Economic pressures often lead to organizations taking greater security risks [21], as systems can be built and launched without appropriate consideration for security [34, 131], or limited budgets are not being spent on the right security controls [149]. There are significant differences between public and private sectors in terms of the **economics** node [33], which were highlighted in Section 2.2.4.

Third party relationships are often established without sufficiently robust contracts [112] that lay down security expectations and responsibilities [37, 106, 92]. Consideration for information security activities must feature highly in the selection of third parties [126], and in the design of systems that are used by third parties, to ensure that control of information assets is maintained [102, 92].

Information sharing with business partners can bring significant business advantages, but as traditional network boundaries become extended, the security of one organization can have a significant impact on another [171]. Non-secure methods of data sharing are one obvious concern [14], but secure connections are just one part of the risk, and strict *need-to-know* principles need to be robustly embedded in information systems [9]. Evidence shows that this can be a retrospective process, as development priorities do not

adequately consider interface requirements [54].

Category	Node	Node Influence
External Factors	Economics	14.88
	Third-party relationship	13.02
	Information Sharing	10.66
	Uncertainty	8.29

Table 5.2: External Factors Domain

The pace of development and the complexity of technology architectures to support collaboration between external teams leads to an **uncertainty** that information security is appropriately addressed [52]. This is a key reason why the EF domain has a strong correlation with the Technology Infrastructure (TI) domain, and this is discussed further in the next section.

5.2.3 Technology Infrastructure

Table 5.3 lists the high-influence nodes for the TI group. On average, the TI nodes showed the greatest correlation with success or failure. By examining these high-influence TI nodes, it was evident that poor **Controls selection** defeat any other security measure [112]. Security needs to be developed into the technical architecture, and this becomes more important as networks grow and become more complex [26].

Organizations can be exposed to greater risks when they adopt complex and unfamiliar technologies [52]. It is therefore preferable to phase the adoption of **new technology** to ensure that it is properly understood, and that adequate resources are in place to support it.

As can be seen in the cobweb diagram at Figure 5.4, the domain that has the strongest correlation with TI is the Business Process (BP) domain.

Implementing technology in a disorganized way, without **standardizing** business processes, will eventually result in a negative impact on security [34]. A lack of testing is also a common cause of IT Security failures [92, 51]. For example, interfacing with external processes and organizations is often considered as secondary to the internal requirements of an information system

[54, 52], but it is also difficult to add this functionality later in a secure way. There can be a trade-off between providing **Interoperability** as quickly as possible, and doing so securely. This is where enterprise security architectures can provide clear benefits and provide accountability [15].

It is also important that the controls selected are appropriately matched to the criticality of the data to be protected, with only the necessary amount of security implemented to control costs and ensure that the architecture of the network is easy to maintain [26, 52]. When implementing and configuring technology, human factors will always have an impact on the success of information security. For example, when selecting security controls, enforcing the **Least privilege** ($r=0.78$) principle will reduce security vulnerabilities [14, 29, 112, 115, 92].

Category	Node	Node Influence
Technology Infrastructure	Controls selection	17.12
	New technology	14.08
	Standardization	13.62
	Complexity	10.72

Table 5.3: Technology Infrastructure Domain

5.2.4 Business Process

As shown in Table 5.4, the business process node has a high influence value of 16.77, and this is mostly attributed to the large number of significant correlations that it has with other nodes (30 total). As can be seen from Figure 5.4, there is a strong correlation between the BP domain and the TI domain, and implementing security technology can be a futile effort if this is not accompanied by clear working practices [52], and automating these working practices is an indicator of the level of maturity in organizations [29].

The BP domain also has a strong link to the HF domain, see Figure 5.4, and user involvement is important when information security is built into business processes [178]. Making information security central to the design of **business processes** reinforces a good security culture [4]. It also pro-

vides a valuable understanding of how new technology will be operated in practice [180], and highlights if previously selected controls are not the most appropriate [2].

Ensuring that there are standard processes in place to recover from security incidents, and that these are constantly tested and adapted by trained personnel, are also key to maintaining **business continuity** [52, 140]. Poor connectivity solutions to maintain **interoperability** in a complex IT infrastructure can allow errors to quickly transfer from one system to another [34, 162] and harm an organization’s ability to quickly recover services in the event of a failure [112]. This is further complicated by multiple vendors who do not support common standards of information security and require workarounds that are not secure, such as copying data out of directory services [112]. Careful design is required to balance the needs of interoperability and information security [15].

Control of the business process is strongly correlated with Enterprise Architecture and is discussed in the next section.

Category	Node	Node Influence
Business Process	Business Process	16.77
	Business Continuity	8.29
	Interoperability	8.00

Table 5.4: Business Process Domain

5.2.5 Enterprise Architecture

As shown in Table 5.5, there are two high-influence nodes in the EA domain, and this is attributed to their association with the success of information security programs, see Figure 2.5 and Figure 5.2.

EAs are designed to ensure that technology, business goals, processes and information flows, and the people of the organization are equally considered [52, 163]. In other words, EAs enforce a **holistic perspective**.

Category	Node	Node Influence
Enterprise Architecture	Architecture	10.07
	Holistic Perspective	8.25

Table 5.5: Enterprise Architecture Domain

Building technology by following a sound EA makes the infrastructure easier to understand and support [26, 131]. An EA provides a top-down approach to understanding the enterprise and informing the selection of security controls [5, 54, 63, 122, 126, 163]. In this way, expenditure on security solutions is easier to justify.

An EA also allows organizations to quickly assess the impact of new vulnerabilities discovered within the infrastructure [5, 55], and helps organizations provide business continuity [163]. Importantly, the EA itself must be easy to maintain, since it will be constantly changing [55], and must be continually updated to the specific needs of the organization [163].

The EA domain is strongly correlated with the SG domain. Whilst the **Framework** node itself does not achieve a high influence value (it is bottom-left in Figure 5.2) and therefore not included here for the EA domain, it does have a strong correlation with the risk management node ($r=0.56$). This is because the governance framework for risk management of the **architecture** needs to incorporate the organizational risks. EA's provide a suitable framework in which to achieve many of the benefits described above [29].

5.2.6 Security Governance

Table 5.6 shows that the SG domain contains many nodes and these have a significant influence on the success of information security. In addition, Figure 5.4 showed how the SG domain has a strong correlation with all other domains. In fact, the combined nodes in SG have a higher average correlation with other nodes ($r = 0.41$) than any other domain. A **business-driven** strategy has the largest influence on successful Security **Governance** (16.71), but many information security programs are not fulfilling business needs [79].

Category	Node	Node Influence
Security Governance	Business-driven	16.71
	Risk management	15.95
	Governance	12.83
	Continuous improvement	11.75
	Timescales	10.41
	Security strategy	8.17
	Security resources	8.04

Table 5.6: Security Governance Domain

Security for security’s sake has limited value to the business, and the organizational context determines the effectiveness of an information **security strategy** [131]. Conducting accurate risk assessments requires consideration for the changing business environment, as well as the technical environment [162]. Assessing the risks to corporate information needs to feature as a key aspect of wider corporate **risk management** [157] and extend across these boundaries [29], but the pace of technological advancement can often mean that technologies are implemented without a full understanding of the risks to the business [9].

An effective information security strategy requires a constant reassessment of information security risks and the **continuous improvement** of controls [11, 84]. This is the familiar Deming Cycle, or PDCA (plan–do–check–act) cycle [126], and requires that the security strategy is sufficiently dynamic to keep pace with the rate of business and technological change [52].

An effective IS strategy requires both an understanding of business and human factors, along with sound technical knowledge and experience. The high cost and lack of availability of competent security personnel (i.e., **security resources**), particularly those with technical knowledge and experience, can make this prohibitive for some organizations [52].

Security Governance must also consider corporate **timescale** pressures. Technical project teams are often psychologically driven to shortcut security standards to meet the demands of business executives, despite knowing that their actions might contravene security policy [34].

These issues highlight a significant challenge for security governance. The

SG domain's highest correlation is with the MI domain, and this is described in the next section.

5.2.7 Management Influence

The MI domain has a very strong correlation with the SG domain (e.g., the **Management influence** and security **Governance** nodes, where $r=0.77$ or **Monitoring** and **Continuous Improvement**, where $r=0.59$) but many organizations are not managing their information security risks, and in some cases, have not fully identified them [29]. A failure of management to assign responsibility for the ownership of corporate information [92], or to understand how their business operates [136], can often be at the root cause of security breaches.

The quality of executive support and continuous **monitoring** are significant factors in achieving successful information security [163]. Unfortunately, most executives regard information security as an administrative matter [126]. The MI domain has a strong correlation with the HF domain (e.g., **Supervision** and **Human Factors**, where $r=0.65$), but a good security culture cannot be commanded; it must be "shaped and directed" (influenced) [71, 153]. Without this commitment, business leaders are unlikely to achieve the results that they desire [122]. While training is arguably one of the most important factors compared to other security measures [163], it is only one part of a wider security program [115]. Employees must be encouraged to transfer their security awareness training to the work place [178].

In an analysis of motivation and deterrence [71], it was found that employees may not always know what the organization's expectations are. It confirms employee negligence as a cause in many costly security breaches but suggests that employees often regard security policy as discretionary, more like guidelines, and may choose not to comply with security policies for reasons of convenience. Employees are also influenced by the attitudes or actions of their peers [71]. The pressure to comply with these subjective norms (e.g. 'well, everyone does it this way') can be greater than what people truly believe is right or wrong.

Without supervision, employees may not be motivated to follow security policies and procedures, so they might as well not exist [178]. This is significant because employees, when left to themselves, often underestimate the security risks associated with their actions, such as transmitting personal information insecurely [122].

Category	Node	Node Influence
Management Influence	Managed	15.98
	Monitoring	15.33
	Management influence	12.05
	Supervision	8.33

Table 5.7: Management Influence Domain

5.2.8 Human Factors

As shown in Table 5.8, the HF domain contains the individual node with the highest influence on the success or failure of security programs (19.84). It is also the domain with the highest number of node influence scores ≥ 8.0 (see Table 5.8). The **Human factors** node occupies the top right hand position in Figure 5.2.

Category	Node	Node Influence
Human Factors	Human Factors	19.84
	Knowledge	16.48
	Internal threat	12.80
	Controls operation	12.09
	Communication	11.84
	Accountability	11.84
	Culture	10.79
	Accidental	8.48

Table 5.8: Human Factors Domain

The **Knowledge** node has a high influence value and this is mostly due to it having the highest number of medium (moderate) correlation values ($r \geq 0.5$) with other nodes (11 in total). However, the **Internal threat** is the

most significant aspect in security failures, see Figure 2.5. Legitimate users can cause data loss, either **accidentally** or maliciously [136]. Insufficient attention is often paid to the human factor, when designing information systems [92]. In fact, users may be unable to comply with policies (i.e., **controls operation**) to carry out normal business processes [183].

A good security culture needs to be carefully shaped and directed [153]. Personality types can affect how compliant individuals will be in terms of following security policy and a study has shown that different levels of emotional stability can affect how individuals decide to take risks in relation to compliance with security requirements [83]. Therefore, the performance of individuals in terms of supporting the organization's desired security culture, and their understanding of the social norms [71], is something that requires continuous assessment [51, 153].

Communication has a strong correlation with the success/failure node(s) and also with other nodes. Several of these other nodes are within the MI domain, as can be seen in the cobweb diagram in Figure 5.4 and mentioned in the MI domain description above. Whilst management may communicate the message that information security is everyone's responsibility, they may be cultivating an environment in which it is no one's responsibility, as there is no **accountability** [52]. Management influence has a key impact on employees' attitudes [174], and will sway the security **Culture** ($r=0.53$).

The HF domain has a strong correlation to the TI domain. In my study, this was particularly associated with selecting controls that provide least privilege, such as role-based access control (RBAC) [29, 112, 92].

5.3 Pairwise analysis of strongest node correlations

To identify the key information security issues that need to form part of a continuous assessment and discover how these issues are related, I conducted

pairwise analysis of the coding².

Strong pairwise correlations were used for this process. These are correlation coefficients that have a moderate or stronger correlation of $r \geq 0.5$, as defined in Table 2.6.

In this section, I describe how I conducted more detailed analysis of the pairwise relationships to determine exactly how these actions and events are related. A summary of these strong pairwise correlations is shown in Table C.2 in Appendix C and are labeled as *Items*.

I linked together the nodes with the strongest correlation coefficients. The resulting figure highlights a chain of events or activities that influence each other and I refer to them as *chains of influence*, see Figure 5.6. The dotted line nodes shown in Figure 5.6 are not high-influence nodes, but they have a strong correlation ($r \geq 0.5$) with an high-influence node.

For example, *Human factors* is associated with the *Internal Threat*; which needs *Supervision*; to enforce *Accountability*. Or, how *Human Factors* can lead to *Accidents* when trying to achieve *Interoperability* for the purposes of *Information Sharing* for *Third Party Relationships*. Therefore, to help reduce *Human Error*, we would most likely need to strengthen our supervision of employees and/or ensure a continual review of business partner arrangements. Similarly, *Documenting security Knowledge* into repeatable *Business Processes* that enforce the *Operation of Controls* can also help to reduce *Human Error* situations.

Figure 5.7 illustrates the concept of the *chains of influence* using a few examples that span the 8 domains. These relationships are relevant both within and across the 8 domains. I first illustrated the relationships across domains in my cobweb diagram (see Figure 5.4).

For example, the green arrows in Figure 5.7 show how an *Internal Threat* is closely associated with the security *Controls Operation* (Item 60 in Ap-

²Although I had already planned to conduct the pairwise analysis, my review of Lean Six Sigma showed that this technique is promoted for the Analysis phase of DMAIC [59]. I described DMAIC in Section 2.3.3.2.

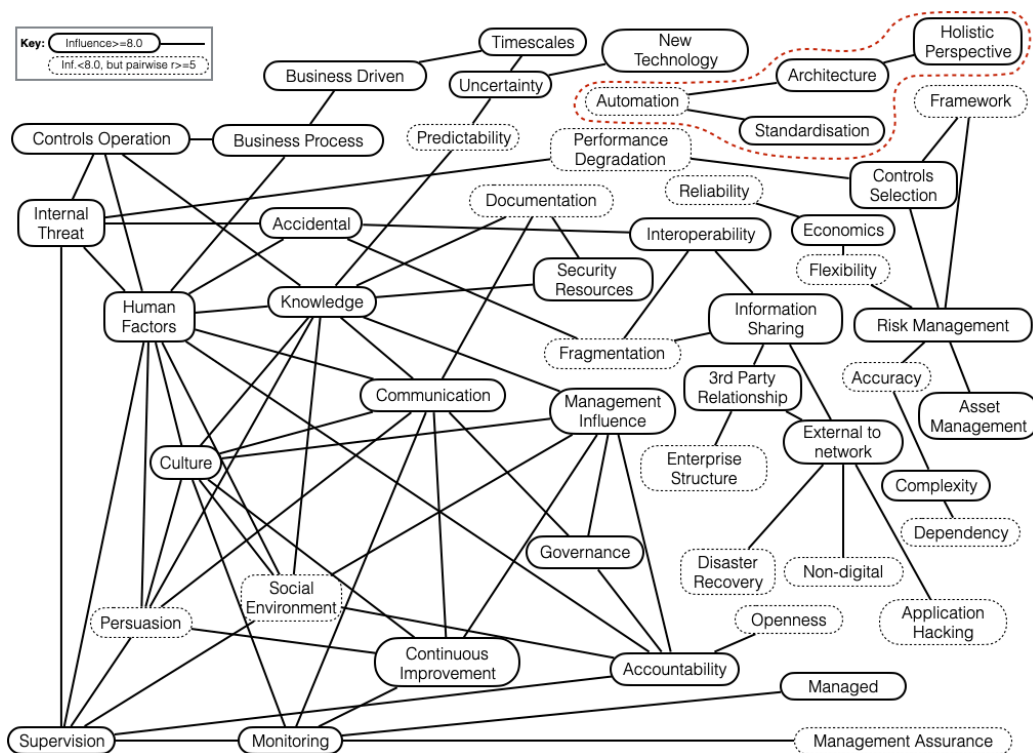


Figure 5.6: Nodes that have a strong influence value, or have a moderate or greater correlation to a strong influence node

pendix C). However, the *Controls Operation* is itself closely correlated with *Human Factors* and there is a *high* correlation ($r=0.73$) between the *Internal Threat* from *Human Factors*. Human behavior often creates an intentional or unintentional *Internal Threat* (Item 47 in Appendix C).

But this can be mitigated, as some of the example pairwise correlations indicated by the green arrows go on to show. For example, the *Human Factor* is affected by a strong security *Culture*, (Item 76 in Appendix C) which requires *Monitoring* (this is Item 79 in Appendix C) to ensure that the culture is being properly *Managed* (this is Item 47 in Appendix C).

Also, the *Social Environment* will influence the security *Culture* (Item 81), so close *Supervision* within peer networks will ensure that the correct training and work attitude is being applied (Item 46).

Good *Asset Management* is key to conducting accurate *Risk Management* as it makes the important business impact a key consideration (Item 1) when

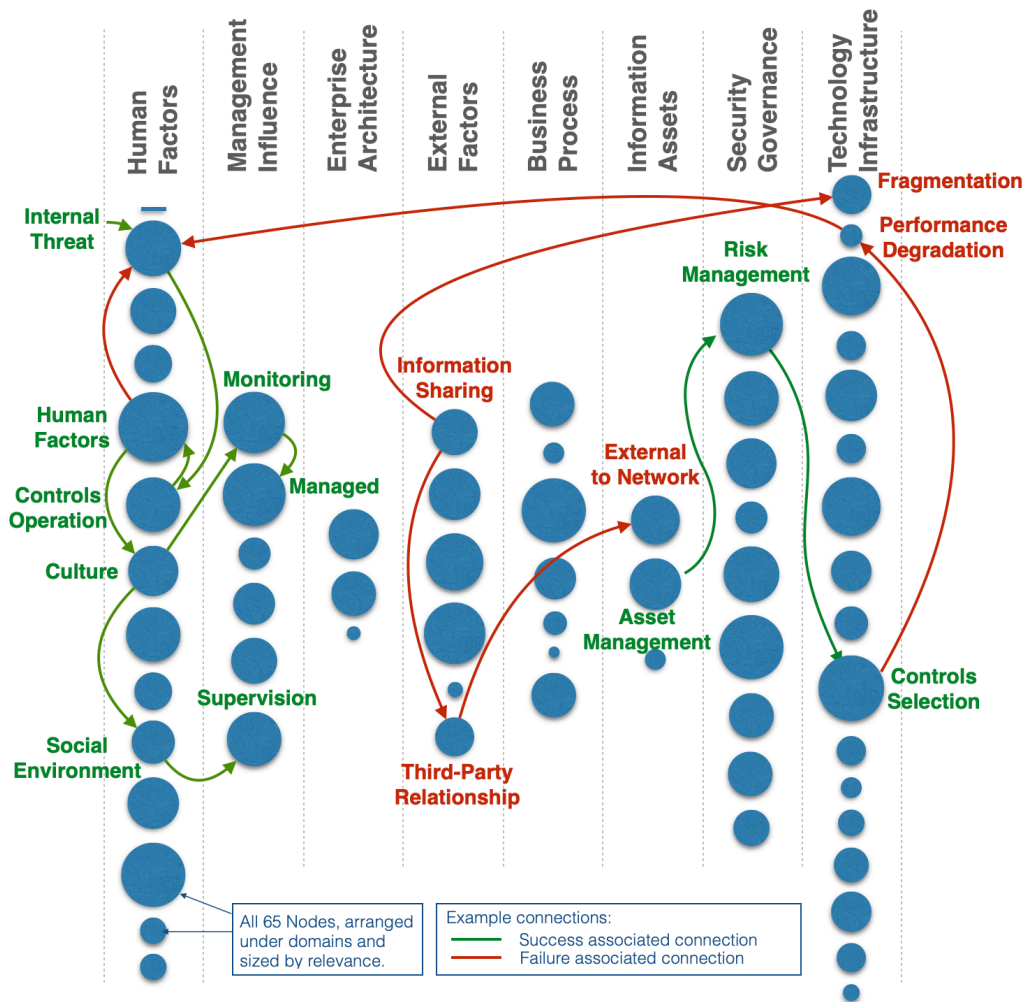


Figure 5.7: Examples of the pairwise correlation analysis

making security *Controls Selection*. However, if the correct selection of security controls is not made, this can lead to *Performance Degradation*, such as making user authentication a difficult process for users (Item 17). This in turn creates an *Internal Threat* as users try to circumvent the drop in their productivity (Item 56) that this causes.

Analysis of the correlations also uncovers important factors that can lead to security failures. For example, see the red arrows in Figure 5.7. When

Information Sharing is conducted within a *Third Party Relationship*, separate data pools are often created to enable the operation of new third party systems or processes. This can lead to *Fragmentation* (Item 11) and the removal of data from the organization's own systems (Item 9), thereby losing control of company data and increasing its attack surface as a result.

Despite including EA in the search criteria of my systematic literature review, architectural references in the literature were limited and theoretical. As such, my analysis has shown that EA frameworks are isolated from other findings of information security failures/successes.

Figure 5.8 shows the nodes correlated with *Architecture* and they can be seen isolated inside the red dotted line area (this is an extract of Figure 5.6, which showed the strongest correlated pair of nodes).

It is evident how isolated EA is from other nodes in terms of their correla-

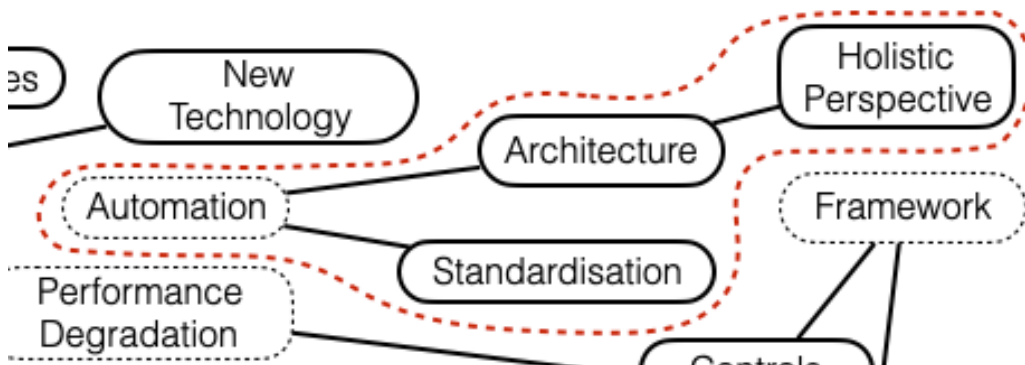


Figure 5.8: High-influence and correlation for architecture-related nodes

tion with success/failure. If EA concepts remain largely theoretical or aimed at producing detailed EA artifacts, then this might remain the case. *Architecture* was highlighted as being significant for success in ISM (see Figure 2.5) but the literature identifies very few associated nodes and this group is largely isolated - only joined to *Standardisation* by including a significantly correlated but low influence node, *Automation* (with $r \geq 0.5$). This is relevant to my study, since it indicates that the theoretical benefits of EA are not explicitly reflected in the literature, suggesting that EA's practical benefits

are not widespread.

5.4 5 Maturity Levels

Analysis of the *chains of influence* showed that the details behind the nodes consist of separate activities that need to be conducted in a structured and ordered way.

For example, consider the *Business Process* domain. Stakeholders need to understand what **business** processes are affected by a change before they can determine how the **change** affects their current information processing. The **impact** of the change is then risk assessed, and this may identify the use of a new third party to assist in carrying out the process (CAESAR8 will check for this). If a third party is involved, then the security **strategy** should include confirmation that a third party contract has been established and includes the protection of the stakeholder's information.

An assessment may be unreliable if it determines that a change to a third party contact is or is not required without fully understanding changes to information processing.

A similar order exists across the other seven CAESAR8 domains, but the order also relates to factors between the domains. For example, a stakeholder must be aware of what information systems are used to process information before they can reliably determine the impact of a proposed technology change.

As part of the process of creating the CAESAR8 checklist, I reviewed all the chains of influence. As a result, I identified that five *maturity* levels were required to ensure that items were completed in the correct order (note that they are only described as maturity levels in the sense of establishing readiness to go live with proposed IS changes). The five levels are shown in Table 5.9.

Step	Level	Description
1	The business	Aspects of the current business that are impacted by a given business change
2	Business change	The nature of the business changes that are planned
3	Security impact	The information security risks in relation to the change
4	Security strategy	The security approach to mitigating the risks of the change
5	Optimization	Actions that improve the organization's future resilience to information threats

Table 5.9: The five CAESAR8 levels

It became evident that all of the pairwise relationships were focused across these distinct levels. Table C.2 in Appendix C contains the full details of how pairwise analysis led to defining these levels. The table includes the level(s) for each individual pairwise reference item (shown in square brackets after the reference summary). The level indicated is the an assessment of which CAESAR8 level the information is most applicable to in the development of the model. All items included one or more of the levels.

Figure 5.9 shows how the pairwise references in Table C.2 are distributed across the CAESAR8 levels.

Level 4 refers to the *Security Strategy*, so most of the references refer to this level, but all levels are represented, and all references are covered by the 5 levels. It is clear from the graph that assessing the *Security Impact* (Level 3) of business changes and *Optimizing* solutions (Level 5) for the future are important factors in the analysis and these considerations have been made an integral part of my artifact.

All 5 levels are relevant across each of the 8 domains, and together they form the individual steps of a CAESAR8 assessment process. Identification of the 8 domains and 5 levels now described a matrix for the model, and the structure is shown in Table 5.10.

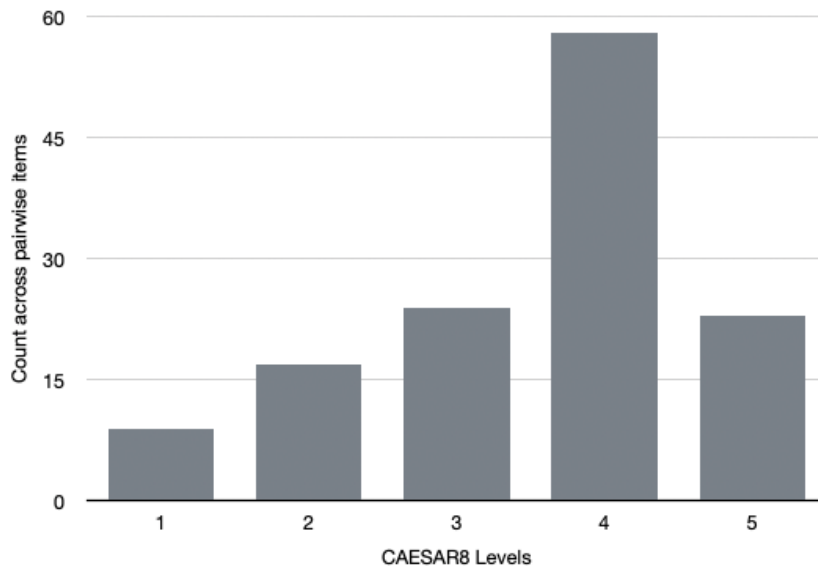


Figure 5.9: Count of the CAESAR8 levels identified in the pairwise analysis

	Business	Business Change	Security Impact	Security Strategy	Optimization
Maturity Level	1	2	3	4	5
External Factors	EF1	EF2	EF3	EF4	EF5
Security Governance	SG1	SG2	SG3	SG4	SG5
Business Process	BP1	BP2	BP3	BP4	BP5
Information Assets	IA1	IA2	IA3	IA4	IA5
Technology Infrastructure	TI1	TI2	TI3	TI4	TI5
Human Factors	HF1	HF2	HF3	HF4	HF5
Management Influence	MI1	MI2	MI3	MI4	MI5
Enterprise Architecture	EA1	EA2	EA3	EA4	EA5

Table 5.10: Basic structure of CAESAR8 matrix

The 8 domains form the rows of the table, and the 5 levels form the

columns. Together, these define a 8x5 matrix consisting of 40 cells. The analysis of the pairwise references identified the contents for each cell. These are the Performance Markers that form the CAESAR8 checklist.

5.5 Performance Markers

The Performance Markers are the 40 questions that make up the questions for the checklist in the CAESAR8 matrix. Having identified the basic structure of the CAESAR8 matrix, see Table 5.10, the references for the *chains of influence* were studied to identify the most important events that should become performance marker questions for each cell in the matrix. This formed part of the detailed study of the pairwise analysis, see Table C.2 in Appendix C, which summarizes the key literature references.

This work was completed in unison with the definition of the CAESAR8 levels to ensure that key factors were addressed in the correct order to ensure the reliability of ISRM decisions.

Figure 5.10 shows the final CAESAR8 matrix and includes the individual performance markers for all eight domains and all five levels of the CAESAR8 model. Each row represents one domain, and each column represents one maturity level.

All performance markers need to be reviewed by each stakeholder during the CAESAR8 assessment³. The final wording of the performance markers includes a generic reference to *stakeholder*. This allows instantiations of the model to use a regular expression to change the wording of the performance marker to the specific stakeholder undertaking the assessment. In this way, it will be clear that the assessment needs to be conducted from the perspective of the stakeholder.

The CAESAR8 assessment is performed column-wise, assessing all domains for a maturity level before moving to the next level. Although performance markers in higher levels can still be reviewed, each assessment must re-check

³This is the design principle, although a few performance markers could be excluded for non-specialist stakeholders and these are discussed later.

CAESAR8 Matrix v2.0	The Business Level 1	Business Change Level 2	Security Impact Level 3	Security Strategy Level 4	Optimization Level 5
EF: External Factors	Stakeholder is compliant with relevant legal, regulatory and corporate requirements	Stakeholder is aware of their dependence on third-party organizations	Stakeholder has checked for any consequential changes to security threats	Stakeholder's budgets are adequate to meet security control changes	Stakeholder believes threat intelligence is optimized in relation to this change
SG: Security Governance	Stakeholder has reviewed all security risks related to the business area under change	Stakeholder's critical objectives for the change, incl. timescales, have been shared	Security and stakeholder risk management methods are aligned, e.g., risk appetite	Security controls and residual risks are agreed with stakeholder	Stakeholder confirms change removes any implicit trust and adheres to least privilege concepts
BP: Business Process	Stakeholder has assessed the criticality of their business processes that are affected by this change	Stakeholder has clarified all resulting changes to information processing, including sharing	Risks of the changes to stakeholder's business process(es) have been determined	Stakeholder has agreed new security measures for process changes, incl. 3rd party contracts	Stakeholder confirms standardized and harmonized processes. Static processes digitized
IA: Information Assets	Stakeholder is aware of their information that is affected, and this is mapped to systems	Stakeholder has reviewed any requirement to move data out of core systems	Changes in stakeholder security risks for data transmission, retention and storage are shared	Stakeholder has agreed all requirements for protecting their information post change	Data integration initiatives are underway from stakeholder perspective
TI: Technology Infrastructure	Stakeholder is aware of all networks and systems potentially affected by this change	Changes to technology are confirmed with stakeholder, incl. use of any external services	All required changes to technical architecture have been confirmed with stakeholder	Stakeholder confirms that testing is documented and executed satisfactorily	Stakeholder confirms modularization (loose coupling) of systems to increase flexibility
HF: Human Factors	Stakeholder identified all personnel operating the current process(es) (internal and external)	Stakeholder has identified their personnel that deliver or support the change	Stakeholder has reviewed the results of user impact analysis for all changes	Stakeholder agrees program for recruiting and training all applicable resources	Stakeholder confirms automation of processes to reduce human error
MI: Management Influence	Stakeholder is aware of the active involvement of the owner(s) of the data and processes	Stakeholder has appointed responsibility for monitoring security compliance	Stakeholder accepts documented requirement to monitor security compliance	Stakeholder has the means to monitor all security controls and respond appropriately	Good security culture evident for stakeholder
EA: Enterprise Architecture	A reference architecture covers related business segments from stakeholder perspective	Draft artifacts describe the transitional target architecture for stakeholder's changes	A full security impact assessment covers transition from stakeholder perspective	The security strategy includes all architecture changes required by stakeholder	Documentation for the reference architecture includes stakeholder

Figure 5.10: Final CAESAR8 Matrix - version 2

the performance markers starting at level one.

The performance markers in the CAESAR8 matrix provide a systematic and repeatable assessment of how security decisions are progressing for any business change program as iterations develop. Symptoms of information security failures often show in the higher maturity levels, particularly for human factors, which makes defining the supporting lower maturity levels a critical step that requires constant review. For example, user training is important (HF4), but before that, critical steps are user impact analysis (HF3) and establishing monitoring functions (MI3). Without an element of user impact analysis (HF3), the business cannot be certain that users are actually able to comply with new security policy and procedures, or if it will even be effective (MI3) in their normal duties [109].

The CAESAR8 model is based on a holistic perspective of key information security success factors within business change projects. The five levels are

based on logical project stages and enforce a review of the business area under change to assess the security impact and strategy. Level 5 (optimization) encourages a review of the longer-term security impact of the change and provides a degree of future-proofing for the organization.

Assessments must continue across all levels for the duration of the project, to ensure that the effects of all changes are fully considered. A project iteration can cause an increase or decrease in CAESAR8 levels, depending on the change and treatment of information security risks. A drop in level merely reflects a healthy review process, and not necessarily a lowering of security performance.

5.5.1 Answering the performance marker questions

The exploratory literature review that I conducted on metrics in Section 2.3.6, found that *existence metrics*, using an extended RAG status (Red, Amber, Green) to answer the performance markers, is the most suitable way to present the results of the CAESAR8 assessment. In the final artifact, each stakeholder completes assessments from their own perspective by choosing one of the following six values when answering each performance marker:

- Yes (Green)– from the assessor’s perspective, this performance marker is relevant and has been met;
- No (Red) – whilst relevant, this performance marker has not been met;
- Partial (Amber)– the assessor wishes to indicate that work in the area of this performance has started but is not complete;
- Trust (Blue) – the assessor trusts that this performance marker is being met by another stakeholder (evidence not confirmed);
- N/A (Black) – the performance marker is deemed Not Applicable;
- (unknown) (Gray) – the performance marker remains unanswered

CAESAR8 assessments should be completed by many stakeholders, independently, and in parallel. The results of these assessments can be very

different. This is an important feature because it ensures that all points of view are captured and no important factors are being assumed. Importantly, the performance markers in CAESAR8 are designed to encourage individual thinking within a stakeholder’s frame of context, rather than encouraging a standardized response that risks quashing individual knowledge.

5.5.2 Presentation of CAESAR8 results

After the stakeholder has completed their assessment, the performance marker values are compared with those of other stakeholders and a single set of results are calculated. The results need to be in a format that is easily shared and understood by all those concerned with the project. Having studied options in my exploratory literature review, see Section 2.3.6, I decided that a radial design is the best format for the artifact. This is shown in Figure 5.11.

Each track sector represents a performance marker and these are arranged

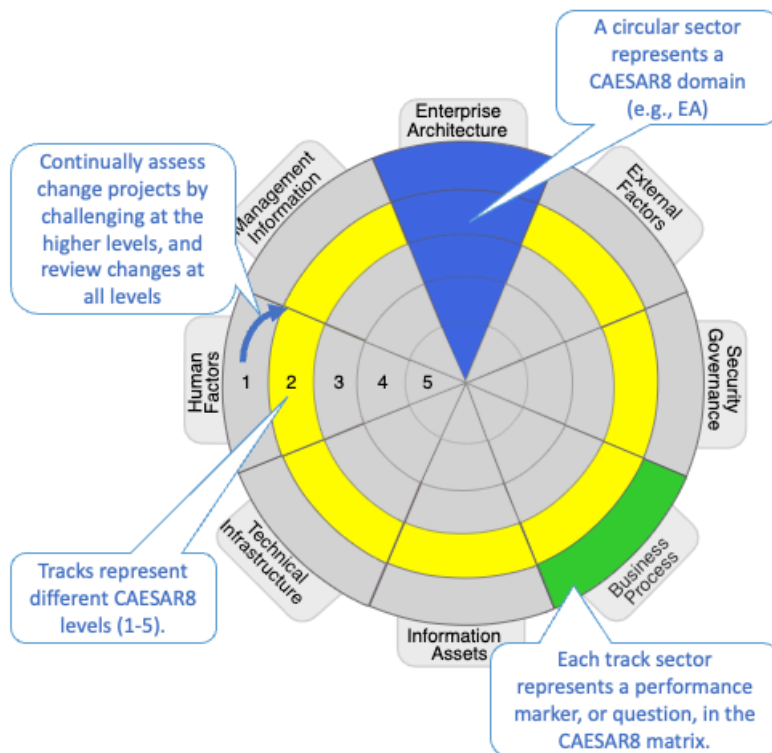


Figure 5.11: Results presentation for CAESAR8

in 5 tracks that correspond to the maturity levels, starting at level 1 on the outside, with one sector for each of the eight domains. The track sectors are colored according to the collective response to each performance marker. Valid responses in this final version are: Yes (green), No (red), Partial (yellow), Trust (blue), N/A (black), and (unknown) (grey).

The radial design allows easy identification of issues and signifies that CAESAR8 is a continual assessment through all levels, as it is a circular, not a linear process. The five levels can be regarded as maturity levels, as each level will only be achieved if all the level's track sectors are continually assessed as being met (Yes – green) or have been specified as not applicable (N/A – black).

5.6 Conclusion of Root Cause Analysis

The root cause analysis process included quantitative pairwise analysis of all nodes to determine their affects on: i) the success or failure of ISRM processes; and ii) on each other. These two factors were combined to produce an overall *influence* value.

High influence nodes were qualitatively analyzed and from this I determined that eight domains were required for the CAESAR8 model. These domains are contrary to the six interrogative categories (6Ws) of familiar architecture frameworks that I originally expected to support. If I had not followed a *first principles* approach for this analysis, the limitations of some commercial EA framework designs may have been less obvious.

The high-influence node literature references were analyzed in more detail to determine the key *chains of influence*. These chains identified that the CAESAR8 model required a second dimension in the form of five levels to provide an ordered arrangement of a set of forty performance markers, or key checklist items, for assessing the performance of ISRM in business change projects. Since the CAESAR8 checklist contained two dimensions, I called this the CAESAR8 matrix.

This matrix forms a tractable checklist that all business stakeholders can use and has been designed to uncover the key information security issues that can lead to a failure of ISRM, even when good IS resource is made available. My general study of checklists identified how such a simple concept already provides a significant improvement to risk management in industry, as demonstrated by aviation and medicine for example. Whilst information security standards and maturity models remain a valuable and important reference, my research identified that they do not provide the same tractable function as the CAESAR8 matrix.

I determined that *Existence metrics*, in the form of an extended RAG status, gave the most appropriate response to the forty performance markers and that a radial design is best for presenting the results. However, this simple RAG system was encouraging a consensus to be reached on the *red* or *green* value of some performance markers. After deciding that I needed to help avoid this mode of thinking in the final iteration of the CAESAR8 model, I extended the RAG response to include a *Trust* element. This change now allowed a wider and more diverse group of stakeholders to answer honestly and, therefore, improve the accuracy of CAESAR8 assessments.

Chapter 6

CAESAR8 design and development

I completed five *design and development/demonstration* iterations of the DSR process to design the CAESAR8 model; an artifact that meets the objectives of all twelve design goals and thus should help to address the fifteen common problem areas and heed the nine underlying issues identified in my systematic literature review.

I have evolved the CAESAR8 model gradually and systematically by applying my findings following reviews and analysis of the literature. The design and development iterations of CAESAR8 have taken the model from early concepts to prototype versions. The iterations are summarized in chronological order as:

- Iteration 1: Concept cyclical design for information security risk assessments
- Iteration 2: Concept model using 8 architecture domains
- Iteration 3: Prototype of the CAESAR8 model with integrated checklist
- Iteration 4: Prototype for combining multiple CAESAR8 assessments using a configurable tolerance value
- Iteration 5: Prototype of multi-stakeholder CAESAR8 model based on

worst-case consolidation rules

Table 6.1 summarizes all design and develop of the CAESAR8 model.

<i>ex ante</i>			<i>ex post</i>	
<i>Concepts (ACVs)</i>		<i>Prototypes (APVs)</i>		
Iteration 1	Iteration 2	Iteration 3	Iteration 4	Iteration 5
<i>Research</i>				
Literature Review; Agile/Lean; 6Ws; Systems Thinking; visualization	Quantitative analysis of coding; Qualitative analysis of coding	Pairwise analysis of coding; checklists; metrics	Cognitive Diversity. Adding a tolerance level to results	Behavioral science for group decision making, i.e., groupthink
<i>Design</i>				
Radial Design; Business to Technology focus	8 domains	5 maturity levels; 40 Performance Markers	Consolidation of assessments. Rules and tolerance variable	Independent review rules; worst-case algorithm with ‘Trust’ option
<i>Instantiation - Product Development</i>				
Diagrams of potential Agile radial model concepts	Conceptual model diagrams	Build assessment in Excel and use VBA to present results	Create Excel Consolidator to combine multiple Excel assessments	Develop Cloud-based, multi-user web app exemplar
<i>Demonstration and Evaluation</i>				
Diagrams for researcher analysis	Peer reviews	Real and synthetic case studies	Real case study (incl. OT)	Real case study; final ex post evaluation

Table 6.1: Overview of CAESAR8 model design, development and evaluation

Table 6.2 summarizes how the design goals for the CAESAR8 model have been addressed by each design and development iteration of the artifact.

#	Essential Design Goals	- Iteration -				
		1	2	3	4	5
Design focus						
1	Base on a non-linear design that encourages continuous re-assessment of changes	X	X			
2	Progression must reflect dependencies between deliverables	X	X			
3	Allow integration into project management processes or operate stand alone		X	X		
4	Fully embrace Agile values	X		X		
5	Encourage just-in-time updating of EA artifacts			X		
6	Focus on the key issues that prevent common IS failures		X	X		
Usability focus						
7	Provides an easy to understand, repeatable checklist			X		
8	Easy to complete assessments			X	X	
9	Quick to conduct assessments			X		
Governance focus						
10	Help to prioritize project work		X		X	
11	Ensure all business departments' perspectives are represented				X	X
12	Easy to interpret and share results at all management levels		X			X

Table 6.2: Design iterations of the artifact and how they address the Design Goals

This chapter describes the design and development of the CAESAR8 model (DSRP Steps 3 and 4), starting with the final CAESAR8 design from iteration 5. The chapter then describes the earlier working prototypes (APVs), iterations 3 and 4, followed by the initial concepts for the CAESAR8 model (ACVs), iterations 1 and 2.

The prototype models are demonstrated by real and synthetic case studies.

6.1 Final CAESAR8 model design principles

As a result of completing five design and development iterations, I have identified five novel design principles that should be observed when creating a model that will provide an holistic but agile solution for the continuous assessment of information security risks during ongoing business change projects. These are the CAESAR8 model design principles and they are all incorporated into the CAESAR8 web app exemplar, which was developed to support the ex post evaluation. The five design principles are described below.

6.1.1 Principle 1: Base model on a practical, holistic design.

Rather than base the model on a commercial enterprise architecture framework that may not provide a proven agile solution to ISRM, design a practical model that allows all stakeholders involved in a business change project to participate in a continuous review of key information security issues as a project progresses.

The CAESAR8 model is designed to allow factors that are commonly associated with the failure of ISRM to be quickly assessed in agile business change projects. The results can be quickly reviewed by all project stakeholders, and remedial action taken where necessary.

6.1.2 Principle 2: Gather multiple stakeholder perspectives.

All business stakeholders that are affected by a business change should be included in an ISRM process to obtain their knowledge and perspectives [129]. In the CAESAR8 model, all stakeholders are guided to provide their knowledge (including tacit knowledge) and preparedness for a given business change in a way that is free from the dangers of *groupthink* [82]. Their assessments are then incorporated into the CAESAR8 model's consolidated final results.

6.1.3 Principle 3: Unify around a tractable checklist.

An ordered and tractable checklist should be used when conducting ISRM for agile business change projects.

For CAESAR8, the checklist examines a common set of enterprise problems that are at the root cause of information security failures. Using CAESAR8, all affected business stakeholders can repeatedly check that these problems are being avoided [148] as a project progresses.

6.1.4 Principle 4: Value process over EA artifacts.

The holistic process for ISRM maybe more important than creating EA artifacts. EA artifacts in general can be difficult to create, difficult to use and a problem to maintain [89], causing delay and expense for projects.

EA documentation is discretionary in the CAESAR8 model. The CAESAR8 model will check that EA artifacts are correctly reflecting the impact of changes in the stakeholder's business area and allows EA frameworks to be accurately *built out* in real-time, if required.

6.1.5 Principle 5: Provide a collective visualization.

The metrics that are used to present the results of ISRM need to be clear and concise to ensure that they can be instantly understood by all project stakeholders.

The results of CAESAR8 model assessments reflect the current findings of all affected stakeholders in relation to a business change. The metrics used provide a shared visualization and supports senior management engagement and intervention [18, 76].

6.2 Ensuring all business departments' perspectives are represented

It is important to capture the knowledge and opinions of all relevant organizational departments in security risk assessments [109] and Section 2.3.7 has also shown how following an EA approach should help organizations to fully understand the security risks associated with a business change.

I searched the literature on associated human behavioral-science to understand the concept of cognitive diversity (described in Section 2.3.4) and the dangers of groupthink (described in Section 2.3.5). This research lead me to refine the design of the CAESAR8 model so that independent stakeholders could conduct the same assessment but from their different perspectives. These individual assessments are then combined to obtain the overall result.

6.2.1 Supporting self-assessments for multiple stakeholders

I had originally envisaged that key stakeholders would have a face-to-face meeting and agree what their responses to the individual performance markers should be after considering the respective views of all business areas. This presents two particular problems:

1. Firstly, it may be logistically difficult to get all stakeholders together for this review. Even online meetings may suffer from geographical time-zone constraints;
2. Secondly, the results of conducting assessments together could easily result in errors of judgment. I explain the reasons for this below.

To resolve both of these problems, I determined that the design of CAESAR8 must allow stakeholders to conduct their assessments independently. Although Kotusev et al. proposed face-to-face meetings with stakeholders for their *Media richness theory* [98], see Table 2.15, my view is that this should be

done after conducting independent assessments, otherwise this risks damaging concurrence-forming when planning EA artifacts. The scientific evidence for this design decision lies in my research into *groupthink*, which was described in Section 2.3.5.

Given the risks of *groupthink* and the pressure in a business environment to conform with the consensus view, I also chose the more pessimistic worst-case rules for the consolidation of assessments. This ensures that the perspectives of all stakeholders are taken into account to uncover important risks to the project.

6.2.1.1 *Trust* other Stakeholders

If stakeholders attempted to answer questions related information security risk on behalf of the entire organization, this would introduce a complication: *What if the stakeholder was relying on the successful completion of a performance marker by someone else but does not expect to see confirmation that this has actually happened?*

Responding with a *Yes*, *No* or *Partial* would be false. To ensure that the assessment was always answered from the perspective of the stakeholder only and to maintain the integrity of the stakeholder’s overall assessment, stakeholders need the ability to express that they were *trusting* that the work will be carried out by another stakeholder. Therefore, the answer “*Trust*” was added to the possible list of responses for each performance marker. Any *Trust* response is shown in the results as a *blue* sector¹ and requires confirmation that it had been completed from the *trusting* stakeholder’s perspective, e.g., by receiving a documented artifact stating the fact or within a review meeting. That stakeholder could then change their response after being provided with evidence. For a more automated handling of *Trust*, stakeholders could be allowed to specify who they are *trusting*, and then the consolidation algorithm could ‘mirror’ the target stakeholder’s response.

¹Note that the *N/A* response was changed from a *blue* sector shown in earlier prototypes to a *black* sector in the final design.

The response should revert back to *Trust* for future iterations unless the stakeholder remains certain that the response provided is still relevant. A key feature of CAESAR8 is that it is the stakeholder’s perspective that must be preserved, so if the responding stakeholder needs to receive evidence that the performance marker is still being met from their perspective, they may well need to see fresh evidence from another stakeholder that has the best knowledge to answer the responding stakeholder’s specific performance marker. It must never be assumed for the latest project iteration.

Answers to performance markers are therefore provided with the confidence that each stakeholder has the appropriate knowledge and experience for their area of responsibility, and for which evidence can be provided to demonstrate true progress. If not addressed appropriately, the problems that lie behind these performance markers often form the root causes of security failures.

6.2.1.2 The consolidation of *Trust* values

When designing the consolidated formula, I gave careful consideration to how *Trust* scenarios should be handled between stakeholders, so that the results are interpreted as expected. My chosen method is to rank *Trust* values more highly in the assessment than *Yes* values. This more pessimistic rule means that if a *Trust* value is present, a *Yes* value will not change the *Trust* result. This ensures that a *Trust* value will not be turned into a *Yes*, unless the original stakeholder changes the value on the next project iteration. However, one or more *No* values for that Performance Marker, will result in a *No* result.

This prevents a scenario where a single stakeholder could turn large parts of the consolidated result to *Yes*, even though they may have no evidence that the ‘trusting’ stakeholder’s concerns have been addressed. The *Trust* value is still different from the *No* value in that it indicates that the stakeholder is reliant on the results of the performance marker but is not responsible for delivering the work that this entails.

6.2.1.3 Final CAESAR8 Checklist

The CAESAR8 *Checklist* for iteration 5 provides a common frame of reference for all stakeholders, regardless of their level of information security knowledge². However, the underlying focus of the performance markers remains unchanged from the earlier prototype CAESAR8 models, since they were developed from the pairwise analysis of the coding, see Section 2.3.2.

The wording of the performance marker questions for iteration 5 are specifically designed to allow the generic term “stakeholder” to be replaced with the stakeholder’s actual description, thereby reinforcing the requirement that responses must be provided from the stakeholder’s perspective only.

In this latter version of the checklist, the EA domain provides important reference to the maintenance of EA artifacts and frameworks. The pairwise analysis did not provide specific references that need to be included from an ISRM perspective only. Only general EA points were discovered, i.e., an holistic perspective is important (item 27 in Table C.2 in Appendix C), the EA process needs to be easy (item 26) and practical tools are needed to guide the use of standards (items 16, 27 & 31). These references serve to underline the need for CAESAR8 as a practical tool. Therefore, the final CAESAR8 matrix identifies optional EA artifacts pertaining to the CAESAR8 level only.

The final version of the CAESAR8 matrix was provided in Figure 5.10 in Section 5.5.

6.2.1.4 Final rules and formula for the consolidation of CAESAR8 assessments

The rules for consolidating the results have been designed to capture a pessimistic view of how stakeholders perceive progress, thereby ensuring that any concerns raised by a stakeholder will be observed. The rules are:

1. If any indicator is set to *No*, then the result is *No*, i.e., the result will

²The performance markers for the EA domain and all of Level 5 are specialist in nature and could be excluded or ‘trusted’ for stakeholders that do not have specialist IS knowledge.

always be *No* regardless of the results of other assessments;

2. If any indicator is *unknown*, then the overall result is still *unknown*, as not all assessments are complete;
3. If any indicator is set to *Trust*, then the result is *Trust*, indicating that stakeholder(s) still need to examine evidence;
4. If all indicators are set to *N/A*, then the result is *N/A*;
5. If at least one indicator is set to *Yes* and the remaining indicators are set to *Yes* or *N/A*, then the result is *Yes* (so any assessment that has *N/A* for this performance marker will not affect the *Yes* result at this point);
6. All other conditions give a *Partial* result.

Based on the above rules, the final formula to calculate the 40 individual summary performance markers is shown in Equation 6.1.

$$\text{Domain}=\{\text{EF,SG,BP,IA,TI,HF,MI,EA}\}, \text{Level}=\{1,2,3,4,5\}$$

$$M = \text{Domans} \times \text{Levels} = \{EF1, SG1, BP1, IA1, \dots, TI5, HF5, MI5, EA5\}$$

$$\forall P \in M.P_v = f(P) = \begin{cases} \text{"No"}, & \text{if } \sum_{s=1}^n P_{sr} > 0, \\ \text{"?"}, & \text{if } \sum_{s=1}^n P_{su} > 0, \\ \text{"Trust"}, & \text{if } \sum_{s=1}^n P_{sb} > 0, \\ \text{"N/A"}, & \text{if } \sum_{s=1}^n P_{sv} = n, \\ \text{"Yes"}, & \text{if } \sum_{s=1}^n P_{sg} + \sum_{s=1}^n P_{sv} = n, \\ \text{"Partial"}, & \text{otherwise.} \end{cases} \quad (6.1)$$

Where:

P is a specific performance marker from the set of 40 performance markers ($P \in M$),

P_v is the summary value of a given performance marker (P),

P_s is a stakeholder's assessment of the performance marker,

n is the number of overall stakeholder assessments and,

t is the *risk tolerance* value expressed as a percentage.

$$P_{su} = \begin{cases} 1, & \text{if } P_s = \text{"unknown"} \\ 0, & \text{otherwise} \end{cases}$$

$$P_{sv} = \begin{cases} 1, & \text{if } P_s = \text{"not applicable"} \\ 0, & \text{otherwise} \end{cases}$$

$$P_{sr} = \begin{cases} 1, & \text{if } P_s = \text{"No"} \\ 0, & \text{otherwise} \end{cases}$$

$$P_{sg} = \begin{cases} 1, & \text{if } P_s = \text{"Yes"} \\ 0, & \text{otherwise} \end{cases}$$

$$P_{sb} = \begin{cases} 1, & \text{if } P_s = \text{"Trust"} \\ 0, & \text{otherwise} \end{cases}$$

6.2.2 Web application

To demonstrate the operation of the final multi-user CAESAR8 model, where many stakeholders independently complete their own CAESAR8 assessments that are then combined into a single overall result, I decided to develop a cloud-based web application. This platform was used to support a hands-on ex post evaluation of the CAESAR8 model by industry professionals.

The web app uses the Azure Application Service hosted in the cloud and Azure Table storage to store structured NoSQL data at the back-end, via JSON (JavaScript Object Notation) web APIs (Application Programming Interface).

I built the application in ASP.NET Core (Microsoft’s open-source web framework) using Razor Pages (dynamic web pages). I used Microsoft Visual Studio for the Mac as the integrated development environment (IDE), and the web app is coded in Javascript and C# 7.0.

The web app uses Scalable Vector Graphics (SVG), with CSS3 (Cascading Style Sheets version 3) and HTML5 (a markup language used for structuring and presenting content on the World Wide Web). This enables me to display the results in the model’s specific graphical form. SVG uses Extensible Markup Language (XML)-based vector image format for two-dimensional graphics with support for interactivity. The SVG images for the model were embedded into the Razor pages in Visual Studio and behaviors were controlled from Javascript procedures. The model’s XML files were created using Inkscape, which is an open-source vector graphics editor.

The web app works in most common browsers, including on smartphones and tablets, although it was not specifically developed to support mobiles. The web app was tested using the desktop versions of Google Chrome, Mozilla Firefox, Apple Safari and Microsoft Edge.

When designing the web app, I made the decision to replace the generic term “stakeholders” in the Performance Marker questions with the specific stakeholder’s identity using regular expressions (regex). For example, instead of “Stakeholder has reviewed..”, the web app will ask: “Sales Manager has reviewed”, or “..from the Finance Manager’s perspective”. This encourages the stakeholder to provide their assessment from their perspective only, and not try to guess or summarize the response for the organization as a whole. This is important to achieve accurate results when their assessment is combined with other stakeholders.

The web app uses two separate pages for operating the model, and the screens for these pages are shown in Figure 6.1 (Appendix F contains full screenshots of the web app).

The first page (*Assessment Page*, Figure 6.1a) contains the assessment for a given project and stakeholder. This contains the performance markers with the stakeholders response and any supporting notes. The second page

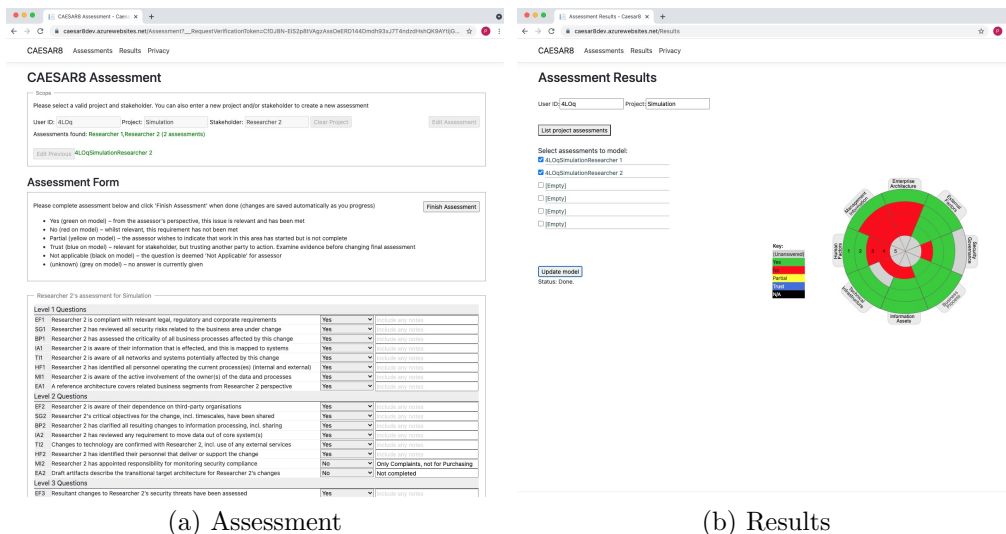


Figure 6.1: Main user input screens of the CAESAR8 web app

(*Results Page*, Figure 6.1b) is where the results are displayed in the radial model. In this page, participants can select which stakeholder assessments they would like to combine for a given project, and then can click the “*Update Model*” button to update the results graphic with the consolidated results. I decided to provide a button to update the model manually, as opposed to automating this from the stakeholder list, so that participants could complete their changes to the selection and then observe the corresponding change in the results when they were ready.

The UML diagram for the basic assessment and results is shown in Figure 6.2. As can be seen from the diagram, the assessments selected by the user for consolidation can be varied across the available stakeholders for a specific project. This enables the user to conduct an element of *sensitivity analysis*. Further, the resulting visualization is transient, in that no results are stored. This is important, because the consolidation must be carried out in real-time, using the very latest stakeholder assessments.

The consolidation function is an important characteristic of the evaluation

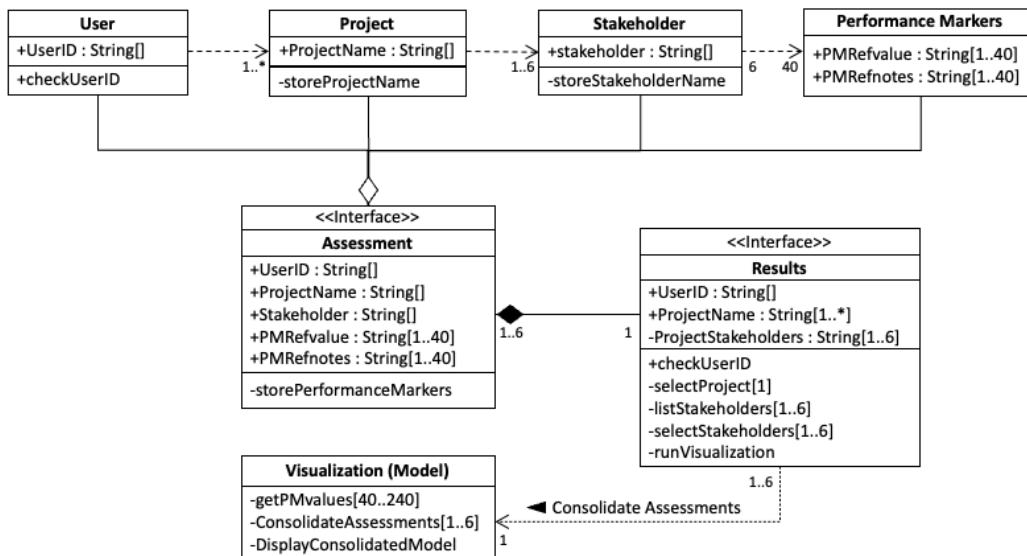


Figure 6.2: UML Class Diagram for the CAESAR8 web app

of the model, so that the user can test how the final results are affected by different stakeholders. As described above, calculating and displaying the results is triggered from a button in the UI, so that volunteers control when the visualization is updated.

The Javascript code that I wrote for the consolidation function of the web app is shown in Figure 6.3. This code consolidates the assessments selected by the user and offers an example of how the consolidation formula shown in Formula 6.1 can be implemented.

Note the order of evaluating the consolidated Performance Marker values matches the formula, and must include a *break statement* if a condition has a boolean value of *true*.

The web app's home page, shown in Appendix F, contained information about the model, guidance for the evaluation and a *defaults* box to make data entry more convenient for volunteers.

```

// Loop through array and count totals of each value;
valQ = 0;
valYes = 0;
valNo = 0;
valTrust = 0;
valNA = 0;

for (var i = 0; i < comparevals.length; i++) {
    ival = comparevals[i];
    switch (ival) {
        case "?":
            valQ = valQ + 1;
            break;
        case "":
            valQ = valQ + 1;
            break;
        case "Yes":
            valYes = valYes + 1;
            break;
        case "No":
            valNo = valNo + 1;
            break;
        case "Trust":
            valTrust = valTrust + 1;
            break;
        case "N/A":
            valNA = valNA + 1;
            break;
    }
}

// compare values to work out single collaboration value - valnow
// alert(valQ + "," + valYes + "," + valNo + "," + valTrust + "," + valNA);
if (assessmentsSelected.length == 0) { //i.e. no assessments selected at all!
    valnow = "?"
} else {
    if (valNo > 0) {
        valnow = "No";
    } else {
        if (valQ > 0) {
            valnow = "?";
        } else {
            if (valTrust > 0) {
                valnow = "Trust";
            } else {
                if (valNA == assessmentsSelected.length) {
                    valnow = "N/A";
                } else {
                    if (valYes + valNA == assessmentsSelected.length) {
                        valnow = "Yes";
                    } else {
                        valnow = "Partial";
                    }
                }
            }
        }
    }
}
// alert("Result: " + valnow);

```

Figure 6.3: Javascript code to implement the consolidation formula

6.3 Implementing the final multi-stakeholder CAESAR8 model

This section discusses some of the requirements for a successful implementation of the CAESAR8 model, such as operating principles (including princi-

ples that management must observe), and guidance on selecting stakeholders.

6.3.1 Using CAESAR8 in Agile projects

EA frameworks typically focus their attention on producing EA artifacts (documents) [98]. However, the agile concept is an important initiative for breaking down the traditional top-down style of leadership where instructions are documented and passed down for execution.

Agile requires a more flexible style of delivery for business change projects that is less dependent on comprehensive documentation.

CAESAR8 provides a novel approach to EA implementation, by enforcing a holistic review process that fully supports the agile values [17]. CAESAR8 supports the four Agile values by design (see Table 6.3).

Value	Agile Manifesto value	CAESAR8 characteristic
1	Individuals and interactions over processes and tools	Values people pulling together their knowledge to ensure that they remain focused on the most important issues at the right time, rather than relying on experts conducting a rigid, and often detached, process.
2	Working software over comprehensive documentation	Values a solution that constantly reviews the latest real-world attributes together, rather than producing outdated documentation in relative isolation.
3	Customer collaboration over contract negotiation	Values the constant collaboration of key stakeholders to ensure the emerging opportunities and issues are addressed appropriately as the solution matures.
4	Responding to change over following a plan	Values constant change and provides real-time assessments, rather than relying on outdated plans and EA artifacts.

Table 6.3: How CAESAR8 supports Agile values

Figure 6.4 shows how Agile values [17] are embedded into the design characteristics of the CAESAR8 model. CAESAR8 is designed to conduct reviews of information security risks for all types of business change, so it is perfectly suited to agile project implementations.

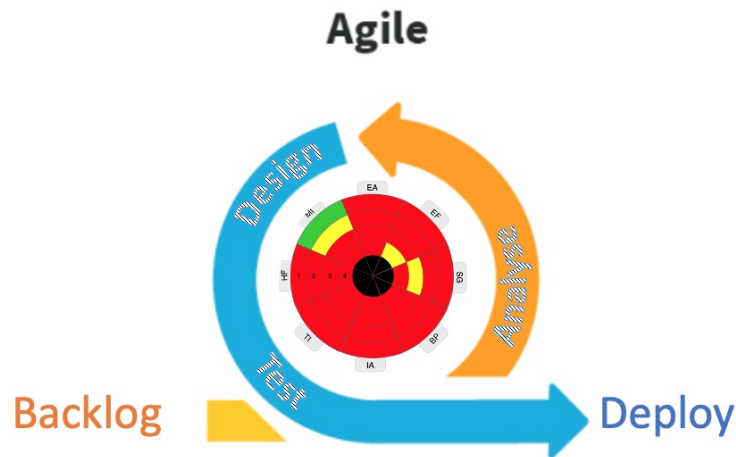


Figure 6.4: Using CAESAR8 in Agile projects

CAESAR8 should be integrated into all aspects of the analysis, design and test phases of project iterations, but it does not impose any specific agile methodologies. This is significant as smaller companies, particularly outside of the software industry, aim to benefit from agile concepts but choose not to adopt all of the agile principles (often due to cost) and choose a hybrid of agile and more traditional methodologies [188].

6.3.2 Selecting Stakeholders

The task of selecting the stakeholders is probably one of the most critical factors for a successful implementation of the CAESAR8 model, as it ensures the most accurate assessments are obtained. In the following sections, I provide guidance for carrying out this important task.

Stakeholders for individual CAESAR8 assessments are selected for their knowledge of the business and/or the change project. If an individual assessment is considered to be inaccurate, CAESAR8 allows for the individual

assessment to be identified and isolated, so that the concerns of that stakeholder can be investigated.

In some cases, an individual stakeholder could be highlighting that a potentially positive effect for the organization that has not been fully considered, e.g., where an associated business process could be automated. This could indicate further opportunities where the project might capitalize.

6.3.2.1 Consider Task for CAESAR8 Assessments

Before describing how stakeholders are selected, it is important to clarify how conducting a CAESAR8 assessment fits into a stakeholder’s normal tasks. Autor et al. [12] describe a formal task model with common business tasks being categorized as either routine or non-routine tasks. A CAESAR8 assessment is a non-routine task, as many stakeholders would only perform this function as an additional task alongside their existing work, usually on an ad-hoc basis. In some cases, this may be a one-off task for a stakeholder.

Autor et al. [12] then describe tasks that demand flexibility, creativity, generalized problem-solving, and complex communications as cognitive tasks that require information processing, as opposed to manual tasks. These two distinct categorizations form a 2 x 2 matrix:

Routine Cognitive (information processing)	Non-routine Cognitive (information processing)
Routine Manual	Non-routine Manual

Table 6.4: Task Categorization

CAESAR8 is concerned with the non-routine cognitive tasks (top right in Table 6.4), where stakeholders are expected to interpret how the performance markers are progressing in an agile project in relation to their own environment. These are precisely the tasks where Page [129] expects the maximum bonus from diversity to be achieved. As the focus of CAESAR8

assessments is on the cognitive diversity amongst stakeholders, the model purposely avoids the risk of team member influence that I describe in Section 2.3.5.

If we were selecting a team of diverse individuals for a creative task, we would have to accept that it is not possible to test for this type of creativity [129]. However, this is not problematical for our needs. CAESAR8 is not particularly intended to select designers in agile projects (although this may have additional value, especially in exploiting opportunities). The primary objective for CAESAR8 is to select stakeholders based on their knowledge of the business process.

6.3.2.2 Choosing Stakeholders and not Influencers

In my study of information security cultures, see Section 2.3.7, I discussed how middle management (representing the group tiers) is key to ensuring an effective security culture operates throughout an organization. CAESAR8 can assist with this objective in two significant ways:

1. It encourages that assessments are carried out by multiple stakeholders, typically in the middle management tier; and,
2. It ensures that a business change project includes the key requirements necessary for management to communicate and monitor information security performance. This is primarily achieved through the Human Factors (HF) and Management Influence (MI) domains.

As mentioned above, the primary objective for CAESAR8 is to select stakeholders based on their knowledge of the business process. However, this must be someone who possess first-hand knowledge of how an affected business process works. They must be the real stakeholder in the project, and not be responding to the assessment in the third-person. They must be the person that can verify the truth in their area of the business with absolute clarity. To do this the stakeholder must possess the knowledge and experience of the business area and not be someone who simply *knows* the basic *facts* in relation to the business area.

For example, actual knowledge allows a stakeholder to determine how information assets will be affected by the proposed business change, and how changes might be influenced by the involvement of third parties. They will know how their business area will be impacted by the timescales; or how staff training programs will impact at a critical time for the business.

Including a more diverse group of experts ensures that more perspectives, experiences and interpretations are considered, resulting in the likelihood of a greater accuracy in predictions. CAESAR8 helps ensure that the key security risks that need to be considered for any change project are more likely to be identified using the collective expertise of a diverse group of stakeholders. This is consistent with the findings that diverse groups solve problems more effectively than homogeneous groups [130]. The diversity of an individual's perspective and heuristics, relative to the other members of a group of problem solvers, may be more valuable than the ability of that individual to solve the same problem on their own [75].

Consider the simple Venn diagram shown in Figure 6.5 that depicts three broadly diverse business groups: Business (e.g., Sales Team), Technical (e.g., IT Department) and Security (e.g., Information Security Team). I will use this basic structure to illustrate the process for selecting stakeholders, although in reality, the groups involved in any given business change can be far more granular. However, the basic rules remain the same.

The stakeholders are best selected from the *symmetric difference* of these sets (groups) minus the full intersection of all three sets. In mathematical terms, this can be expressed in set builder notation. The potential set for selecting the full set of stakeholders (x) would be:

$$\{x|x \in (S \Delta T \Delta B) \wedge x \notin (S \cap T \cap B)\} \quad (6.2)$$

This rule means that we are specifically avoiding any of the intersections. For example, it is possible to find seemingly ideal stakeholders that are in these intersections and could cover multiple groups, such as the specific asset owners inside a business department, or security liaison officers within

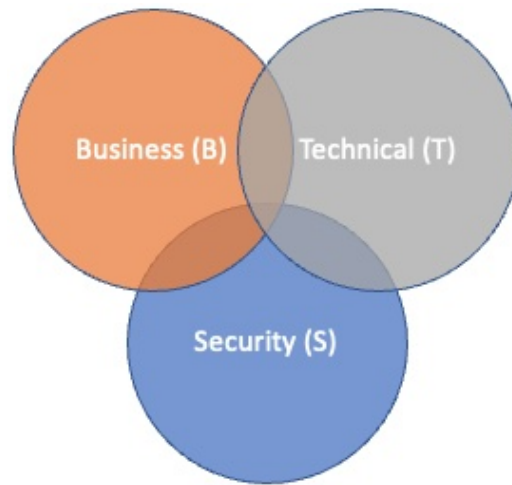


Figure 6.5: The example set of three organizational groups

a business group that have been tasked with liaising with the information security team, or a technician from the IT department assigned to a particular business group. However, these roles will not normally offer the greatest diversity, even if they seem to offer the best knowledge of all groups. Their experience will have been shaped to some degree by their experience in their main group. They may lack some of the day-to-day experience of other team members, or a potential conflict of interest might skew the results. They could still be included if they have crucial knowledge, but must not cover more than one perspective on their own.

The number of stakeholders, n , is difficult to quantify, but generally the more genuine stakeholders that are involved in the CAESAR8 assessments, the more truthful the results are likely to be. Critical to this however, is that they have a very specific relevance to the business change project under assessment. In other words, they have a true stake in its success (they can be directly or indirectly effected by the change, but it is important not to confuse *stake* with *responsibility* because that can encourage inaccurate assessments).

Stakeholders must be selected from all relevant groups that have been identified. Therefore, if three stakeholders are selected from the three groups used in the example, i.e., $n=3$, and we use the following notation for these groups:

X_1 is group S , X_2 is group T , and X_3 is group B ; then the following rule applies:

$$\forall i \in n. x_i \in X_i \tag{6.3}$$

Where x_i is an individual stakeholder in the set of stakeholders (x), i.e. $x = \{x_1, x_2, x_3\}$.

In other words, it is important to select the three stakeholders from each of the three groups identified in the example: i.e., exclusively Security, Technical and Business. There can still be additional stakeholder assessments that are added to this selection. The design of CAESAR8 consolidation process will ensure that any concerns of a particular stakeholder are highlighted. In reality, there would be a far greater number of groups included in the selection than I have shown here. The simple *Business* group particularly may be divided into Sales, Design, Manufacturing, Distribution, and so on. Maybe there are further subdivisions of these groups to find the right stakeholders. Importantly, the selection process must be cognizant of the specific needs of the change project and not based on the organizational structure. The stakeholders are not heads of department, but are likely to be middle managers or practitioners. The organizational structure is largely irrelevant to this process and risks not capturing important stakeholder assessments.

Greater involvement of stakeholders in the risk assessments for business change projects also encourages greater engagement and ownership of the associated challenges for these stakeholders. I know from my literature review, as well as my own experience within the industry, that effective information security culture cannot simply be enforced on a business. It requires collaboration and a shared understanding of the risks and risk tolerances across the whole organization, together with agreement and understanding on how to safely reach a shared goal. This takes time to achieve, as it relies on the benefits of collaboration being seen to work across the organization, where

everyone's opinion matters.

In my section on Further Development Opportunities, see Section 8.5, I describe how a fully functional or commercialized version of the CAESAR8 model could allow stakeholders to propose other stakeholders that should be approached for an assessment. This is additional to the requirements described in this section, and should not be implemented as a substitution function.

6.3.3 CAESAR8 Implementation principles

CAESAR8 reviews are carried out by all stakeholders independently, to review the business change from their individual perspectives. To ensure the best results when introducing CAESAR8 assessments into an project, some CAESAR8 implementing principles need to be followed:

1. All relevant stakeholders for a change project must be identified, and a separate CAESAR8 assessment conducted from their perspective alone. The stakeholders will be individuals or groups with full, hands-on knowledge of how the business operates in their particular area.
2. Answers to CAESAR8 questions must always be given from the stakeholder(s) perspective only, and never generalized, or guessed, for the organization.
3. Senior management must not influence individual assessments, but must encourage and review the results of assessments conducted by individual stakeholders who possess an accurate and up-to-date knowledge of the business. Senior management should review the unaltered, consolidated assessments as part of their decision making process.
4. The final results of CAESAR8 assessments should be shared with other stakeholders (but not before all assessments have been completed).
5. The sharing of all stakeholder assessments and results should take place before any meeting or discussion is held to resist concurrence-seeking.

6. For maximum benefit, CAESAR8 assessments should be conducted on a continuous cycle through all maturity levels, so that the correct levels of maturity can be reestablished at every product iteration.

In this way, everyone is made aware of the issues and potential vulnerabilities, but without influence. A meaningful discussion can then take place to address any concerns that emerge.

6.3.4 Case Study - multi-stakeholder demonstration of the Gangs Matrix

This case study was used to demonstrate the multi-stakeholder characteristics of the CAESAR8 model. It makes use of an enforcement notice published by the Information Commissioner's Office (ICO) in 2018 [36], which details an investigation into a data breach. The ICO's report has already determined that there were significant problems associated with the implementation of new technology and a corresponding change to working practices.

6.3.4.1 Background

In an ongoing effort to reduce the serious crimes committed by gangs in London, UK, the Metropolitan Police Service (MPS) desired to prosecute more offenders and also deter young people from engaging in such crime. The MPS published their central strategy for dealing with gang crime in what is referred to as the **Gangs Operating Model**. The implementation of this model falls to the 32 separate local boroughs of the MPS. The Model requires that each local borough creates its own **Gangs Matrix**, an intelligence database, to record details of gang nominals. These are then compiled centrally to form a London-wide matrix. These nominals are members of a gang. However, the ICO investigation reviewed the Gangs Matrix and discovered that it also contained victims of gang crime. The MPS's operation of the Gangs Matrix led to the serious disclosure of gang victims data, and the subsequent investigation by the ICO discovered multiple contraventions

of the DPA that lead to the breach.

My case study is limited to the specific breaches of Principle 7 of the DPA, which relates to information security. There were seven specific findings in the enforcement notice that relate to Principle 7:

1. Excessive information sharing with third parties without any agreement as to how the information needed to be used and protected;
2. A lack of protection of the information that was shared with third parties, and no consideration for the sensitivity of the data in question;
3. The routine transfer of Gangs Matrix information was without appropriate security, such as encryption;
4. The Gangs Matrix allowed local copies of unprotected data to be created;
5. Users of the Gangs Matrix did not have their access revoked when they moved out of gang-related roles;
6. A lack of governance and central oversight allowed poor and unlawful processing of data to go unchallenged; and,
7. A lack of central data protection guidance, and failure to monitor compliance with the guidance specified for the operation of the Gangs Matrix. No privacy impact assessment was ever completed for the system's personal data.

The ICO's findings helpfully provide details of the different perspectives of stakeholders in the Gangs Matrix system.

6.3.4.2 Methodology

For this case study, four separate stakeholder assessments were conducted: i) Central Command; ii) a joint assessment for the Local Boroughs; iii) the

DPO; and iv) the CISO. These four separate assessments were then consolidated using the rules described by Formula 6.1.

The degree of involvement of the Senior Information Security Officer (CISO) and Data Protection Officer (DPO) is not clear from the ICO report. However, I have included these assessments as they were subject matter experts that should have been consulted. Their assessments are important for the demonstration. Although the report describes Local Boroughs in the collective, in reality there could be independent assessments for each borough to ensure that all views and specific work practices are represented.

While the results have been obtained retrospectively, the detailed description of the ICO's findings have allowed the CAESAR8 assessments to be conducted with the necessary confidence.

6.3.4.3 Results

Individual assessments for all four stakeholders are shown in Figure 6.6, along with their aggregated results. I also show the results for the aggregation of the Central Command and DPO to show whether CAESAR8 can identify security risks even if the CISO is not aware of the change project. This ability to select which stakeholders to combine is a characteristic of CAESAR8, and can be used in *what-if* analysis during risk assessments.

The perspectives of the police's head office (Central Command) and local enforcement teams (Local Boroughs) reveal an interesting contrast where Central Command was unaware of the impact that the project would have on the work of the Local Boroughs. Figure 6.6a represents Central Command's perception that the Gangs Matrix solution is fit for purpose and delivering against the Gangs Operating Model, which is the description of how to use the Gangs Matrix database. Several of the responses are marked as *Trust*, because the ICO's notice describes how management were expecting the solution to be a "bedrock" of their "Gangs Strategy". In reality, they had no hands-on monitoring of this fact, and their understanding had not translated into technical solutions and guidance.

CAESAR8 assessments must be completed from the perspective of the

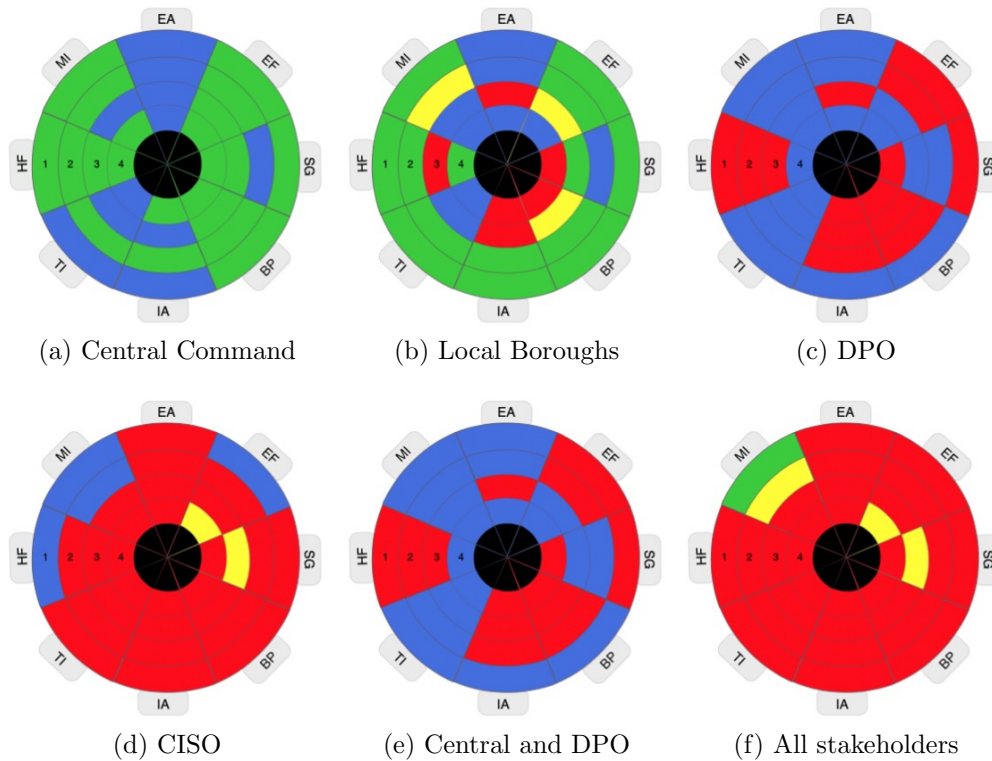


Figure 6.6: Gangs Matrix Assessments - Case Study 3

stakeholder only. The operational stakeholders (Central Command and Local Boroughs) are mostly *green* and *blue* for levels 1 and 2, indicating that there are no specific concerns being raised. However, higher levels show increasing concerns for the Local Boroughs assessment (Figure 6.6b). For example:

- MI2: there is concern within the Management Influence domain at level 2 (MI2), where I have specified a *Partial* assessment. This performance marker specifically states that “[Local Boroughs] has [have] appointed responsibility for monitoring security compliance”, but the ICO finding #6 described the lack of oversight for illegal processing of information at the local level;
- HF3: the Human Factors domain at level 3 (HF3) requires that “[Local Boroughs] have reviewed results of user impact analysis for process and technology changes”. However, the ICO findings #1 through to #4,

are all concerned with the problems that local users were experiencing when working with the database and involving third parties, indicating that an impact assessment cannot have been completed.

- IA4: issues for HF3 have indirectly lead to a problem for the Information Assets domain at level 4 which states that “[Local Boroughs] has [have] agreed all requirements for protecting information post change”. The ICO findings #2 and #7 indicate that the risks were neither considered, nor guidance provided.

6.3.4.4 Discussion on the consolidation of *Trust* values

Using this case study as an example, this section discusses why I chose to perform the consolidation of *Trust* values in the way that I describe in Section 6.2.1.2.

Potential CAESAR8 project stakeholders can clearly be identified from the description given in the ICO’s report. Two of these are likely to have been the Central Command and the DPO (Data Protection Officer). If they had completed their own CAESAR8 assessments, Figure 6.7 shows the probable results.

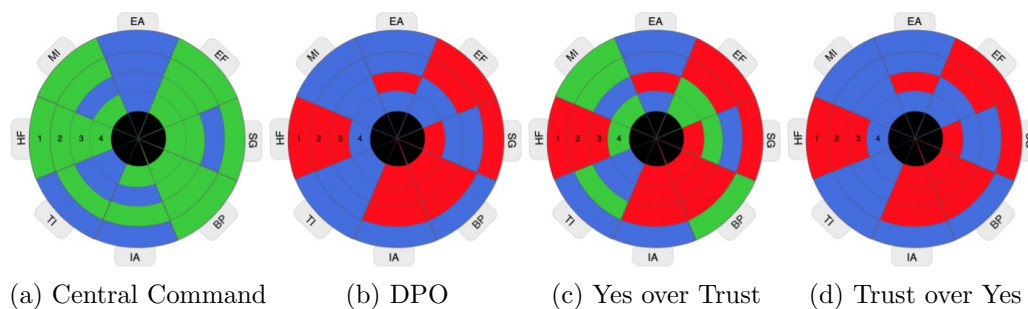


Figure 6.7: The impact of different rules the consolidation of *Trust* values

It can be seen that the results for Central Command shown in Figure 6.7a and that of the DPO, Figure 6.7b, are quite different. When the results are combined, the way that *Trust* values are handled can also give a very different consolidated result. Figure 6.7c shows the results of the consolidation

with *Yes* values taking precedence over the *Trust* values (a *Yes* value will override a *Trust* value), and Figure 6.7d shows the results with *Trust* values being preserved.

The result shown in Figure 6.7d should help ensure that the discussion continues on the areas of concern, which supports the CAESAR8 principle that it is the process that is most important and not the final result. For example, the *Yes* values of BP1 and MI1 in Figure 6.7c could lead a project manager to assume that all stakeholders have now confirmed who owns the data involved in the change and that its criticality has been assessed. This might be the case. However, the real situation could be that, unbeknown to Central Command (who is providing the assessment from their own perspective only), the DPO knows that not all stakeholders have yet been asked to provide an assessment, such as third parties. It is for this reason that the consolidation process formula has been designed to present the more pessimistic³ result shown in Figure 6.7d.

6.3.4.5 Conclusion

The primary purpose of CAESAR8 is to allow competent stakeholders to check whether significant issues have been considered in ongoing projects. This case study has highlighted that security problems can easily exist undetected, or even proliferate, if there are not consistent management checks for good security governance. I therefore conclude that this case study has shown that aggregating the assessments of all stakeholders allows for the full identification of potential issues, which is not possible when relying on individual assessments alone.

When viewing just the consolidated results for Central Command and DPO in Figure 6.6e, it is apparent that the DPO is likely to have expressed caution at the start of level 1. The DPO's concerns have over-ridden the Central Command's more optimistic assessment. The ability to conduct this kind of

³I have discussed potential enhancements to this rule in Section 8.5, where a stakeholder could select an option to *trust* a specific stakeholder as part of a future development.

analysis with the model is a useful feature when treating risks.

6.4 Earlier CAESAR8 prototype models

This section discusses the earlier prototype CAESAR8 models (APVs). Completing the CAESAR8 matrix allowed me to develop the earlier concept model (ACV from Iteration 2) into the first working prototype model for Iteration 3.

6.4.1 Development of first CAESAR8 prototype

To enable me to demonstrate CAESAR8 using a case study, I created a Microsoft Excel instantiation of the CAESAR8 model.

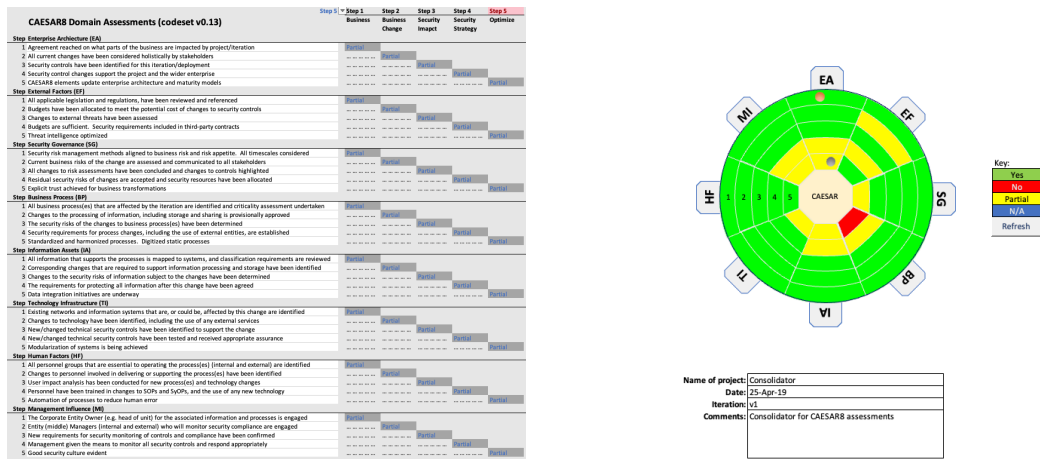
The assessment of the performance markers and the presentation of the results are kept in separate Excel tabs, see Figure 6.8. Keeping the assessment separate from the results helps to support a continuous assessment of the checklist, rather than diverting the assessor's focus onto specific areas that are shown as *amber* or *red*, i.e., where the assessment is non-compliant with a performance marker.

When the assessor has completed all performance markers up to the required level in the *Assessment Tab*, the assessor would then move to the *Results Tab* and click the *Refresh* button to display the results.

The assessment process can be repeated quickly and continuously and, in an operational scenario, would allow resources to be directed to the known problem areas.

6.4.2 Case Study - single assessment demonstration of the Gangs Matrix

The purpose of conducting this case study was to demonstrate the general usability of the CAESAR8 model and also whether it could identify the key security risks associated with a business change.



(a) Assessment Tab

(b) Results Tab

Figure 6.8: CAESAR8 MS Excel Instantiation

6.4.2.1 Background

The background to the case study has already been provided in Section 6.3.4, to demonstrate the final design iteration of CAESAR8. It concerns an ICO enforcement notice that was published in November 2018 which documented an in-depth investigation into the causes of an information security incident. The incident occurred after the introduction of a new system called the Gangs Matrix.

6.4.2.2 Methodology

I assessed the Gangs Matrix from the perspective of a new system under development. To answer the questions for the CAESAR8 model, I used information from the ICO’s enforcement notice, in particular relating to DPA Principle 7 (security). This gave sufficient information for a retrospective assessment to be carried out.

When responding to the performance markers, the assessor has 5 options to choose from in in this earlier (single-assessment) iteration of the CAESAR8 model:

Yes – from the assessor’s perspective, this performance marker is relevant and has been met;

No – whilst relevant, this performance marker has not been met;

Partial – the assessor wishes to indicate that work in the area of this performance has started but is not complete;

N/A – the performance marker is deemed 'Not Applicable';

? – the performance marker remains unanswered

The starting point for the assessment is shown in Figure 6.9. The Excel model calculates the current maturity level, by determining the highest level where all conditions have been met (therefore, the red ball is currently shown on the edge of the model).

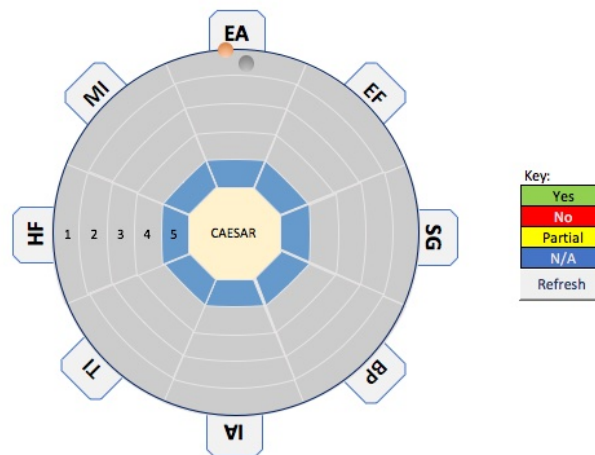


Figure 6.9: Blank Excel CAESAR8 model with level 5 set as not applicable.

I assessed CAESAR8 levels 1–4, but excluded level 5 (optimisation) because not enough information was available to assess this level. I therefore set level 5 to 'Not Applicable' (*N/A*).

6.4.2.3 Results

Each CAESAR8 level of the assessment took approximately four minutes to complete. The final results after completing all four levels of the CAESAR8 model are shown in Figure 6.10.

These results indicate that the project was most likely forging ahead without the involvement of key stakeholders and subject matter experts (SMEs)

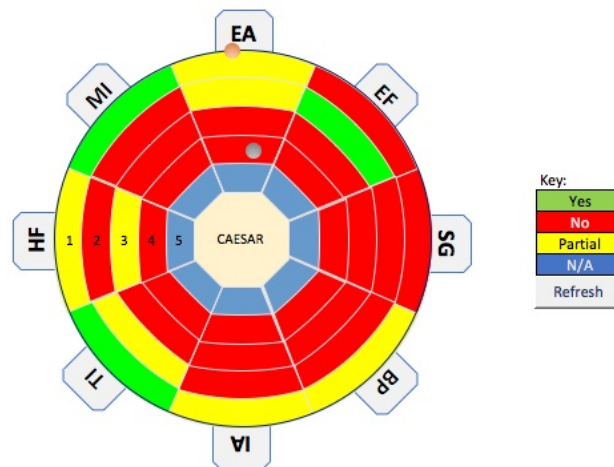


Figure 6.10: CAESAR8 Model Levels 1-4 Assessment for Gangs Matrix

to review the consequences for information processing as a result of these IT changes. This first level of the assessment should already be raising concerns about the level of compliance. Even if the shortcomings of the External Factors (EF) domain was not immediately obvious at level 1, the lack of involvement of the CISO and alignment of information security risk assessments for this business change project (SG1 performance marker), should have been very clear. Limitations around the current understanding of business processing (BP1), the information needs (IA1), and human factors (HF1) should have also surfaced.

The findings go on in latter levels to show a deteriorating assessment from earlier levels (note that in a real-time time CAESAR8 assessment, a re-evaluation of all CAESAR8 levels should be undertaken to identify the effects of all project changes).

It is clear that there was probably very little in the way of effective CISO engagement. For example, the assessment at Level 3 fails in all but one area: HF3. The HF3 assessment has been marked as *Partial*, as some credit has been given for knowing how users will be accessing the Gangs Matrix. However, this could not have considered all local processing needs, such as the sharing of the data (BP2 and BP3). The ICO's findings for items 2 and 3 (listed above in Section 6.3.4 and copied below in Table 6.5) confirm that

technical controls were not mitigating these risks.

For CAESAR8 Level 4, which is the information security strategy, I have determined from the evidence that all responses are *No*. The absence of lower level CAESAR8 security reviews results in a flawed security strategy.

This would have demonstrated unequivocally that further work was required before the Gangs Matrix was safe to go live.

Table 6.5 describes how CAESAR8 would have uncovered all contraventions of DPA Principle 7 (DPP7) described in the ICO’s report.

#	Summary description of ICO’s finding	CAESAR8 Performance Marker
1	Excessive information sharing with third parties without any agreement as to how the information needed to be used and protected	EF1 - checks for legal compliance, e.g., the DPA
2	A lack of protection of the information that was shared with third parties, and no consideration for the sensitivity of the data in question	IA2 - requirements for moving data out of core systems IA3 - risks caused by method of data sharing
3	The routine transfer of Gangs Matrix information without appropriate security, such as encryption	IA4 - protection of data in transmission
4	The Gangs Matrix allowed local copies of unprotected data to be created	BP2 - changes to information processing, such as sharing BP3 - Risks from changes
5	Users of the Gangs Matrix did not have their access revoked when they moved out of gang-related roles	HF3 - security impact of technology changes (e.g. CISO reviewing access control)
6	A lack of governance and central oversight allowed poor and unlawful processing of data to go unchallenged	MI2 - monitoring responsibility appointed MI3 - procedure for monitoring documented

Table 6.5: DPA contraventions mapped to CAESAR8

6.4.2.4 Conclusion

The detailed information provided in the ICO's report has allowed a realistic test of the CAESAR8 assessment to be completed. Using the evidence given in the ICO's report, I found it was easy to answer the CAESAR8 questions quickly and with relative confidence. It took only minutes to review each CAESAR8 level after reading the ICO's enforcement notice and the CAESAR8 Performance Markers identified all seven of the ICO's findings where the Gangs Matrix had serious information security failings.

The Case Study has shown how CAESAR8 can be used to provide a rapid and holistic assessment of information security risks in a business change project at any stage of its development. In this case study, the CAESAR8 model has provided valuable metrics as a standalone assessment. This was achieved without the need for prior security assurance activities (e.g., an accreditation document set) that may have otherwise hindered the agile development.

When used in an ongoing project, CAESAR8 should be used in real-time for each iteration of the project, thus providing valuable feedback on the developing security strategy. CAESAR8 also supports the work of architects, as it prompts for incremental updates to EA documentation.

Even without the benefit of hindsight, completing CAESAR8 assessments during the project should have made it obvious that the project was not considering all processing of the information and was not providing adequate protection of corporate information. CAESAR8 highlights some concerning issues from the very first step in the assessment, and these issues become progressively worse in later steps.

The case study has also shown that even with some false answers, possibly given in good faith (such as Technology Infrastructure TI1 - I made this compliant, as this is all about the new database) should have raised questions when considering these alongside Human Factors (HF), Business Process (BP) and Management Influence (MI), at the same level (i.e., holistically).

6.4.2.5 Known limitations to this early case study

There are likely to be logistical problems in obtaining a consensus view from all stakeholders and subject matter experts (SME) on the value of each performance marker in the CAESAR8 assessment. If there are geographical and/or time constraints in achieving this via face-to-face or even virtual meetings, then a CAESAR8 assessment could actually become a very time-consuming process. This would not achieve a key objective of CAESAR8 (Goal #9 - **Quick to conduct assessments**). Also, if a key stakeholder is excluded from the assessment for any reason, then the loss of that potentially important perspective could limit the accuracy of the overall assessment (missing Goal #11 - **Ensure all business departments' perspectives are represented**). Therefore, this is a crucial problem that required a resolution and this is described in the next section.

6.4.3 Combining CAESAR8 assessments

To resolve the limitations described in Section 6.4.2.5 above, I focused the next design iteration (Iteration 4) on combining multiple assessments to create a single consolidated result. For this, I defined five basic rules for combining the individual stakeholder assessments:

1. If any indicator is set to *No*, then result is *No*
2. If any indicator is set to ? (unanswered), then result is ?
3. If all indicators are set to *N/A*, then result is *N/A*
4. If all indicators are set to *Yes*, then result is *Yes*
5. All other conditions give a *Partial* result.

(Note that there was no *Trust* value in CAESAR8 model iteration 4.)

As can be seen, this is a worst-case scenario; for example, any *No* result will provide a *No* answer.

6.4.4 Adding a tolerance value to the consolidation rules

When I wrote the formula for the consolidation, I also wanted to allow some control over how the result is calculated by introducing an independent variable for risk tolerance. To achieve this, I introduced an independent variable into the formula that organizations can adjust to determine how the results of the CAESAR8 assessments are combined so that, for example, a single *No* result will not change an overall *Yes* result. This example indicates a level of tolerance of risk that is higher than the worst-case scenario. Another way to think of this is controlling a level of error in the results that is considered acceptable, i.e., should only a single *No* results effect the overall results if all other values are *Yes*. A higher tolerance value could be set to ignore a single *No* result.

In simplest terms, the tolerance value will specify how *No* and *Yes* the assessments of multiple stakeholders are handled when they are combined and therefore this can be achieved by averaging the results and comparing this to a independent risk tolerance variable that a user can adjust. This can be calculated by using the arithmetic mean, i.e.,:

$$\frac{1}{n} \sum_{i=1}^n x_{sr} \geq \frac{t}{100} \quad (6.4)$$

Where n is the total number of assessments, s is a stakeholder's assessment, r is a 'No' (red) value for the current performance marker, and t is the risk tolerance value (expressed as a percentage of tolerance in the Excel Consolidator). Therefore, if this condition is True, then the summary result for that performance marker is '*No*'.

Conversely, if the condition is False, then the check continues for a potential 'Yes' (green) result using the following formula (where g is 'Yes' (green) value for the current performance marker):

$$\frac{1}{n} \sum_{i=1}^n x_{sg} \geq \frac{100 - t}{100} \quad (6.5)$$

These conditions determine the results for individual performance markers. Before applying the variable, if all values are *unknown* or *not applicable*, the results are already determined and will not need to be calculated. Where the *No* or *Yes* condition has not been achieved, the default will be *Partial*.

Therefore, the formula to calculate the 40 individual summary performance markers is shown in Equation 6.6.

$$\text{Domains} = \{\text{EF, SG, BP, IA, TI, HF, MI, EA}\}, \text{Levels} = \{1, 2, 3, 4, 5\}$$

$$M = \text{Domains} \times \text{Levels} = \{\text{EF1, SG1, BP1, IA1, } \dots, \text{TI5, HF5, MI5, EA5}\}$$

$$\forall P \in M. P_v = f(P) = \begin{cases} \text{"?"}, & \text{if } \sum_{s=1}^n P_{su} = n, \\ \text{"N/A"}, & \text{if } \sum_{s=1}^n P_{sv} = n, \\ \text{"No"}, & \text{if } \frac{1}{n} \sum_{s=1}^n P_{sr} \geq \frac{t}{100}, \\ \text{"Yes"}, & \text{if } \frac{1}{n} \sum_{s=1}^n P_{sg} \geq \frac{100 - t}{100}, \\ \text{"Partial"}, & \text{otherwise.} \end{cases} \quad (6.6)$$

Where:

P is a specific performance marker from the set of 40 performance markers ($P \in M$),

P_v is the summary value of a given performance marker (P),

P_s is a stakeholder's assessment of the performance marker,

n is the number of overall stakeholder assessments and,
 t is the *risk tolerance* value expressed as a percentage.

$$P_{su} = \begin{cases} 1, & \text{if } P_s = \text{“unknown”} \\ 0, & \text{otherwise} \end{cases}$$

$$P_{sv} = \begin{cases} 1, & \text{if } P_s = \text{“not applicable”} \\ 0, & \text{otherwise} \end{cases}$$

$$P_{sr} = \begin{cases} 1, & \text{if } P_s = \text{“No”} \\ 0, & \text{otherwise} \end{cases}$$

$$P_{sg} = \begin{cases} 1, & \text{if } P_s = \text{“Yes”} \\ 0, & \text{otherwise} \end{cases}$$

The risk tolerance calculations need to be applied for every performance marker when assessing *Yes/No* answers for each of the stakeholders. It can be seen from this formula that changing the risk tolerance value (t) has a significant impact on the overall result, so limits for its value may need to be imposed.

6.4.5 The Excel Consolidator prototype

To test the concept of combining multiple stakeholder information security assessments into a single result, I designed the Excel Consolidator. This is a similar Excel spreadsheet used for the main assessment but with one crucial difference: it also had a tab where all stakeholder assessments could be listed, rather than an editable assessment tab. The consolidator spreadsheet then automatically fetches the separate results from the independent assessment spreadsheets that have been listed, and updates the assessment tab automatically with the combined result.

Figure 6.11 shows the list tab of the consolidator and how it combines each performance marker. Each row is a single assessment, and the top row is the combined summary. The summary is calculated based on the formula described above, Formula 6.6. Below, I show how I have converted this to

an Excel formula, and provide a closer examination of the List Tab.

CONSOLIDATION LIST		risk tolerance when averaging % 50 calculated for number of models: 5		Summary:																																										
Filename	Name of project	EA	EF	SG	BP	IA	TI	HF	MI																																					
CEASAR8Modelv04737MaxBoeingManagers.xlsm	Boeing 737 MAX Example - Boeing Managers	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
CEASAR8Modelv04737MaxBoeingEngineers.xlsm	MAX Example_Boeing Engineers																																													
CEASAR8Modelv04BetaPaper2FAA01.xlsm	MAX Example_FAA																																													
CEASAR8Modelv04737MaxBoeingPilots.xlsm	MAX Example_Pilots																																													
CEASAR8Modelv04737MaxBoeingOperators.xlsm	MAX Example_Operators																																													

Figure 6.11: MS Excel Consolidator *List* tab

How the above formula was implemented in the Excel Consolidator can be seen in Figure 6.12. This screenshot of the formula was taken from the first summary cell shown in Figure 6.13b (column E), where cell D2 is the *risk tolerance* cell (the value of t) shown in Figure 6.13a.; currently set to 50 (%) in this case. Cell D3 is a count of how many assessments are included in the consolidation.

```
=IF(COUNTIF(E7:E20,"?")=$D$3,"?",
IF(COUNTIF(E7:E20,"N/A")=$D$3,"N/A",
IF(COUNTIF(E7:E20,"No")/$D$3>=($D$2/100),"No",
IF(COUNTIF(E7:E20,"No")+COUNTIF(E7:E20,"?")=$D$3,"No",
IF(COUNTIF(E7:E20,"Yes")/$D$3>=((100-$D$2)/100),"Yes",
"Partial"))))
```

Figure 6.12: Consolidation formula

Below is a description of how each line affects the overall result:

1. If all values are *unknown*, then the summary result is *unknown*;
2. If all values are *not applicable*, then the summary result is *not applicable*;
3. If the percentage of *No* values exceeds or is equal to the percentage tolerance value, then the summary result is *No*;
4. If the combined *No* and *unknown* values is equal to the total number of assessments, then the summary result is *No* (this condition has been included because it means that all values that have been changed from *unknown* values have been changed to a *No* value. If this check was not included, the presence of a single *unknown* result will default the consolidated result to *Partial*, even if all other values were *No*. This could create a false impression of progress.);

The subject of this case study was the highly-publicized failure of an Operational Technology (OT) solution in the form of two Boeing 737 MAX aircraft crashes in 2018 and 2019, with the combined loss of 346 lives [39]. The circumstances surrounding these fatal accidents provided a demonstration of how assessing and combining solutions from multiple perspectives can highlight potential problems with security or safety that are inherent in a design proposal.

When conducting the CAESAR8 assessments, I used information from documents that are in the public domain and allegedly describe the cause of the crashes of the Boeing 737 MAX [24]. At the time the case study was conducted, investigations were ongoing. The case study is only used to demonstrate CAESAR8 performance using documentation available in the public domain and should not be used to explain the actual cause of the 737 MAX incident.

6.4.6.1 Background

Efficiency is very important in the air transport business. Boeing needed to compete with Airbus and deliver a narrow-bodied aircraft with larger, more efficient engines. Rather than continue with the development of a new aircraft, Boeing announced a new engine option for its aging 737 airframe, and it called this the 737 MAX. Development and testing of the 737 MAX was rapid, allegedly helped by the fact the Federal Aviation Administration (FAA) had delegated many aspects of the evaluation for certification to Boeing. The Boeing 737 MAX was certified in 2017, and delivered to its first customer later that year. Between October 2018 and March 2019, there were two fatal crashes of the Boeing 737 MAX, and these appeared to have occurred under very similar circumstances. Attention became focused on Boeing's new Maneuvering Characteristics Augmentation System (MCAS), which is the software designed to help prevent the new aircraft from stalling. The aircraft was eventually grounded world-wide.

A summary of the issues that were used for the CAESAR8 assessments:

- The use of the 737 airframe presented problems in mounting the larger engines. This created handling problems.
- MCAS was a software solution designed to counteract the handling problems.
- By using the existing airframe, Boeing was able to shorten the time required for certification with the FAA.
- Using the 737 airframe was advantageous for operators.
- Pilots were unaware of the existence of MCAS initially.
- Boeing allegedly withheld some details of MCAS.
- Pilots could not counteract the trim change made by MCAS using yoke movements.
- If corrected by the pilots, MCAS would repeatedly restore the trim change.
- The power and authority of the MCAS trim changes were considerable.
- MCAS behavior was not modelled in flight simulators.
- Pilot training for the 737 MAX derivative was rudimentary.
- MCAS reacted to data from one sensor only.
- Faults already reported with sensors.
- Sensor disagreement warning was an optional extra.
- FAA delegated safety evaluations to Boeing.
- Boeing's safety assessments may have contained errors.
- FAA under pressure to meet Boeing certification schedules.
- Concerns about FAA's oversight strategy [125].
- Safety concerns about growing levels of automation [135].

6.4.6.2 Methodology

From the above issues, I determined that a separate assessment should be conducted for each of the key entities that were potentially involved in the design and operation of the 737 MAX: Boeing managers, Boeing engineers, operators or airlines, FAA, and aircrew (pilots).

In reality, more stakeholders would have been selected but these are the main entities that are regularly described in the literature and serve to demonstrate this iteration of CAESAR8. Therefore, I have conducted five separate CAESAR8 assessments from these stakeholder perspectives.

6.4.6.3 Results

The results show the individual assessments, followed by the combined results.

6.4.6.3.1 Individual assessments Four of the assessments are shown in Figure 6.15 (I do not show the results for operators/airlines, as the assessment showed all levels as compliant).

Figure 6.15 shows the differences in the CAESAR8 assessment for the individual entities. Level 4 is likely to be the minimum level that safe conditions would need to achieve, and the Boeing managers' assessment of the 737 MAX (Figure 6.15a) indicate that it was suitable for production. Similarly, for the operators/airlines, the situation is all *Yes* (green), since they are already familiar with operating the Boeing 737, for which pilots are already trained on the airframe type.

Level 5 values can largely be ignored, since these are concerned with the optimization of security or safety systems – although it is interesting to note that for Boeing managers, the *No* values (reds) at Level 5 are attributable to Boeing's remaining long-term aims to replace its aging 737 airframe, which are not met by this change.

However, the assessment for Boeing Engineers (Figure 6.15b) and the FAA (Figure 6.15c) shows many problems caused by the issues described above. The *Yes* values at levels 1 and 2 show that changes are understood. How-

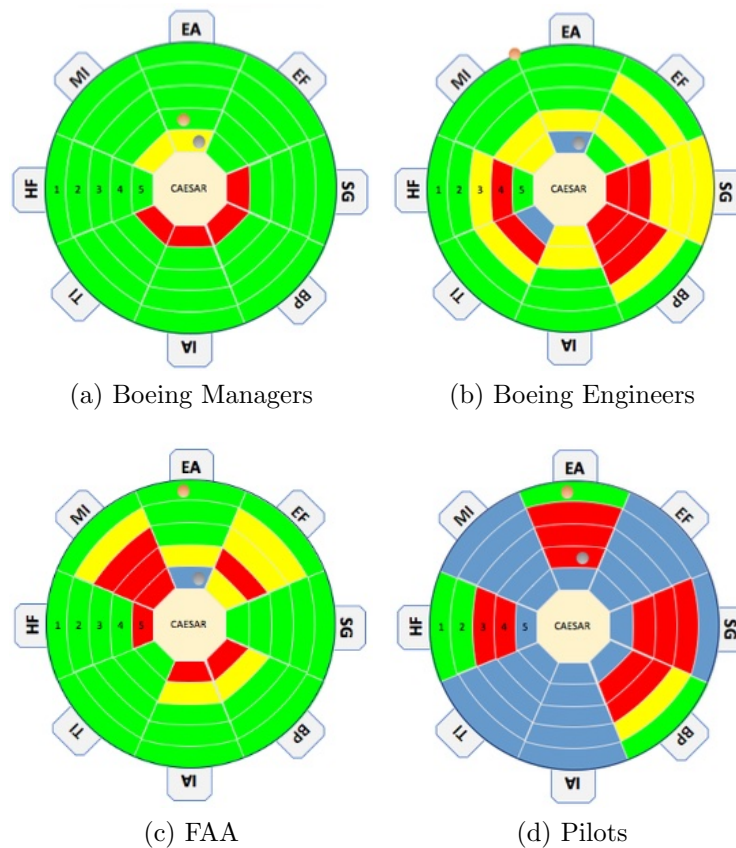


Figure 6.15: CAESAR8 Group results for 737 MAX issues

ever, SG1 issues are attributable to the incongruity between engineering and business risk assessments and the time-related pressures that must have existed for the engineers. This has to be addressed. Particularly notable for the Engineers is the red at TI4, which is down to limitations in the MCAS design, and how that has directly affected the pilots' primary flight control (BP3 and BP4). It seems inconceivable that engineers would not have had reservations with the solution and concerns about the balance of authority between pilots and automation provided by MCAS (HF4).

For the FAA, the reds for MI are due to the FAA's alleged inability to provide an adequate level of oversight. Associated with this has to be the quality of FAA documentation (e.g. IA4).

If Pilots are aware of the same issues, then their likely assessment is also

provided (Figure 6.15d). The pilots group has a number of domains marked as *Not Applicable* (N/A), as their scope has been largely limited to operating procedures and human factors for this assessment. Our assessment is based on pilots being consulted, although that may not have been the case, as explained earlier.

6.4.6.3.2 Consolidator results All assessments, or a subset, can be combined in the CAESAR8 Consolidator. The results of combining all five assessments can be seen in Figure 6.16. As discussed in Section 6.4.3, combining assessments, the consolidator has been designed to allow some adjustment in the results by altering a risk tolerance value. Adjusting the risk tolerance value makes the results appear more pessimistic or more optimistic. The first profile (Figure 6.16a) shows the worst-case scenario, with the tolerance level set low (20% tolerance value) therefore is the result of combining the most pessimistic findings for performance markers across the assessments. This immediately highlights the real extent of the problems that exist with the current solution.

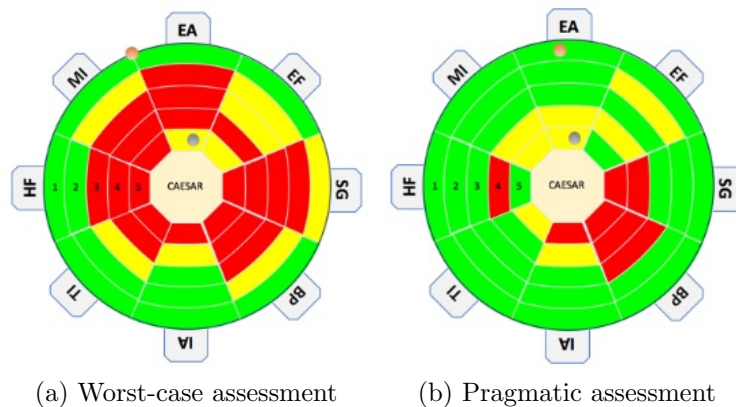


Figure 6.16: CAESAR8 Consolidated results for 737 MAX issues

Figure 6.16b shows a more optimistic assessment (40% tolerance value), which only highlights the most significant issues. I therefore call this result the *pragmatic* assessment.

EF is limiting progress beyond Level 1. In my assessment, this is due to a

combination of budgetary and time-related constraints associated with meeting the challenges of market pressure, such as the time needed to refine and test MCAS software (TI4); train pilots (HF4); and, for the FAA to provide the necessary oversight during certification (IA4).

Issues with the SG domain (i.e., ‘safety’ governance) suggests that conflicts existed between business strategy and engineering solutions. The BP domain issues confirm that operating the changes implemented by the 737 MAX derivative was a potential factor that led to the plane crashes leading to the grounding of the 737 MAX.

This consolidated assessment shows the significance of taking an holistic view of the changes that are being implemented. It also highlights how CAESAR8 can quickly combine the assessments of individual units to provide an accurate assessment of the current overall risk. These two factors support the agile implementation of an architectural perspective when assessing the changing residual security or safety risks within any project.

6.4.6.4 Conclusion

The 737 MAX case study showed a striking difference between the assessments conducted for different interest groups (Figure 6.15). This emphasizes the importance of obtaining a CAESAR8 assessment at each business unit, so that the true risks are uncovered. The CAESAR8 Consolidator can combine individual assessments to provide an holistic view – which in this example provided a total safety picture.

The 737 MAX case study has also demonstrated how CAESAR8 can serve OT and engineering projects, as well as information security projects; and where required, it can also provide an integrated perspective. This is down to the agnostic and EA-focused design of the model’s structure and its performance markers.

Figure 6.16 shows how the risk tolerance variable can change the final results between the worst-case and the more pragmatic result. The assessment has not met the performance markers in both cases. However, the

tolerance value was removed from the final consolidation formula so that all stakeholder assessments are reflected in the consolidated result.

6.4.7 Removal of tolerance variable

The tolerance value was being applied equally to all of the listed assessments. There was no provision for individual stakeholder tolerance values to be included at this point to provide a weighted average, but it already highlights a concern around the opportunities for “gaming the system” [16]. This means that administrators of a CAESAR8 assessment could systematically exploit the risk tolerance variable to obtain the desired result; effectively, removing any undesirable assessments from the consolidated result. Further, introducing weightings would contradict a design goal for the artifact, **Goal #11: Ensure all business departments’ perspectives are represented**. Even keeping a universal tolerance value would have this potentially negative effect on CAESAR8 results.

Therefore, averaging assessment results was removed from the design of CAESAR8 and I decided not to pursue any form of consensus rules (see Groupthink in Section 2.3.5). This is because the objective of CAESAR8 is to identify risks, not to reach a consensus on the final result.

Similarly, I chose not to keep the single risk tolerance variable for the consolidation of stakeholder assessments (Section 6.4.4 described adding this calculation) or introduce a weighting for individual stakeholders because such weightings are imprecise and subjective. These variables could be adjusted on the basis of one individual’s biases and risk hiding important communications from a stakeholder. This 737MAX case study had demonstrated how different the results can be when combining assessments using different tolerance values (see Figure 6.16).

Adding weights to the algorithm will not add any benefit to the CAESAR8 result [42]. I have devised the performance markers in CAESAR8 by analyzing the coding of scientific articles and these provide a valuable prediction that non-experts can now use. Used in accordance with clear operating rules, CAESAR8 should produce a more reliable result than a single expert judg-

ment when it comes to identifying residual security risks in business change projects. Adding any weighting to the results that could be based on one individual's non-optimal prediction would turn CAESAR8 into an improper linear model that would flaw this entire assessment process [42]. Simple, "modest" checklists are better to ensure that concerns highlighted by stakeholders are properly considered and knowledge-loss is avoided [58].

6.4.8 Consistency of CAESAR8 Assessments - a synthetic case study

6.4.8.1 Purpose

A test was created based on a synthetic scenario to review consistency of the results of CAESAR8 assessments when performed by two independent assessors: myself, an Information Security Professional and part-time student; and, an Associate Professor in Computer Science.

Whilst my earlier Gangs Matrix case study had demonstrated how comprehensive the CAESAR8 checklist was, it was conducted by one person only. The synthetic scenario, however, was specifically designed to check how objective the performance markers are and whether two independent assessors could obtain the same results.

6.4.8.2 Method

This case study considered the perspective of a fictitious purchasing department. I created the scenario based on my experience of a typical company change where information could be at risk but the issues do not always reveal themselves in terms that explicitly match the descriptions of CAESAR8 Performance Markers.

The scenario is based on an outsourcing project, as that was a concern uncovered in my systematic literature review that particularly affected public sector organizations in times of austerity⁴.

Both researchers reviewed a fictitious scenario and conducted a CAESAR8

⁴These are potential target organizations who could benefit most from my model.

assessment for a purchasing department stakeholder. The scenario is provided in Appendix G.

6.4.8.3 Results

The results are shown in Figure 6.17. Whilst there are similarities between the independent assessments conducted by the two researchers based on the scenario described, there are notable differences.

The researchers had provided notes to support their decisions for choosing performance marker values, so it was possible to determine the reasons behind the differences. Some of the differences were attributable to the subjective wording of the performance markers in this earlier version of the CAESAR8 checklist but it was also obvious that there were differences in the researchers' own experience of the scenario and the way in which it was presented. These differences were reflected in their assessment.

As an example, when writing the synthetic scenario, my intention was that HF3 was *Yes* and HF4 was *No*. However, the researchers arrived at different results for HF3 and HF4. This was partly due to the researchers having different knowledge about the scenario, but was also because they had a different perspective of information security risks as a result. To ensure a more realistic test, the scenario contained information that required some tacit knowledge of the situation, rather than explicit facts that can be read in the text.

When reviewing evidence for HF3, the scenario described how discussion on the impact for human resources had taken place, although an 'impact analysis' was not explicitly stated. When considering the response for HF4, which includes staff training, past experience of some TUPE (Transfer of Undertakings - Protection of Employment) arrangements might raise concerns that staff training programs were not in place and could be impacted.

Two significant findings emerged:

1. The performance marker questions need to be in plain language and with no ambiguity;

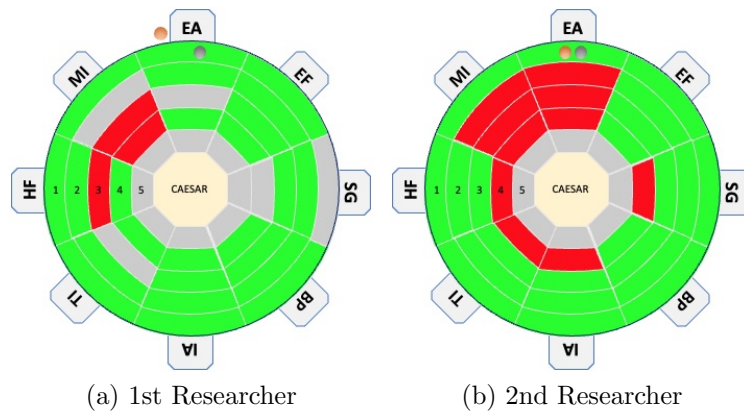


Figure 6.17: Case study results for researchers

2. Differences of opinion, and therefore the results of assessments, may be a valuable characteristic of the assessment that I need to embrace in my artifact.

6.4.8.4 Conclusion

All performance markers were read carefully and edited to make sure that they were objective. These changes were incorporated into version 2 of the CAESAR8 matrix and it is included in Figure E.3 in Appendix E.

More significantly though, this study highlighted a need to capture all relevant stakeholder perspectives and make sure that they were all included in the results. This suggested that further searching of the literature was required to determine how the different perspectives of stakeholders should be treated by CAESAR8 to help ensure the best possible information security risk decisions.

The results of this research were a key contributor for designing the CAESAR8 model in way that captures the independent knowledge of all stakeholders that are affected by a business change project, and combines them into a single result as described in Section 6.1.

6.5 Initial concepts for the CAESAR8 model

The latter iterations of the CAESAR8 model that are described above were working prototypes (APVs). However, the earlier concept iterations of the CAESAR8 model (ACVs) conceptualized the objectives for solving the identified problems, so were significant to the final designs of CAESAR8.

The design decisions for the early concept versions are described in this section.

6.5.1 First concept of a circular model based on 6Ws

The first iteration of the artifact is shown in Figure 6.18. Based on the requirements for a cyclical model, the 6Ws are arranged in a hexagon. The model also has a number tracks (five shown in the figure) that reflect layers in the architecture, and these represent increasing levels of maturity as the security risk assessment progressed. Progression through the model addressed the requirements of each track sector before progressing to the next track, or in other words, the next level of maturity.

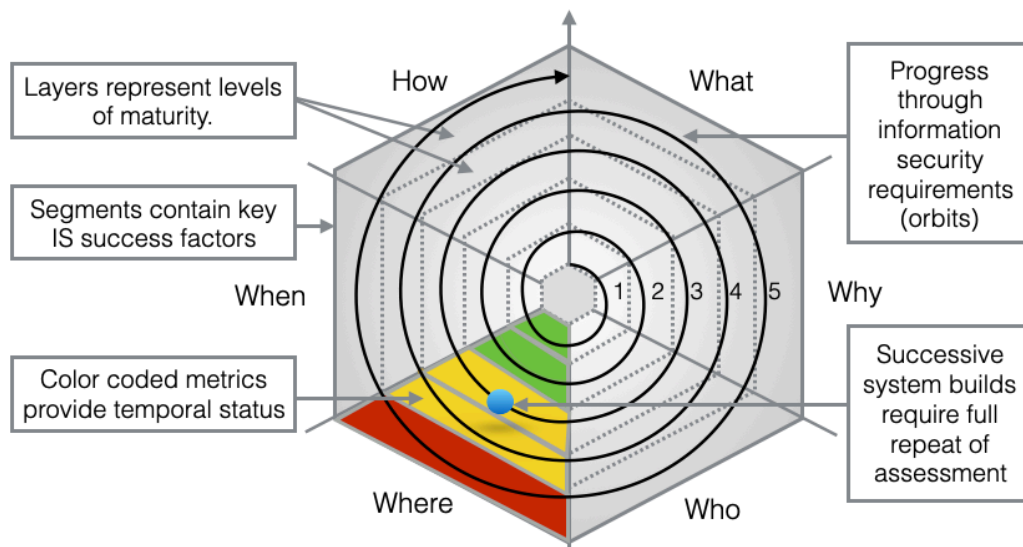


Figure 6.18: First 6Ws cyclical design concept

6.5.2 Second concept with separate strategic disciplines

Another consideration for the early concepts is subdividing each segment of the hexagon into the potentially critical success factors for business strategy, information strategy and technology strategy groupings (the separate strategic disciplines). This concept is shown in Figure 6.19.

This (ACV) model starts from the center and moves out to higher levels to

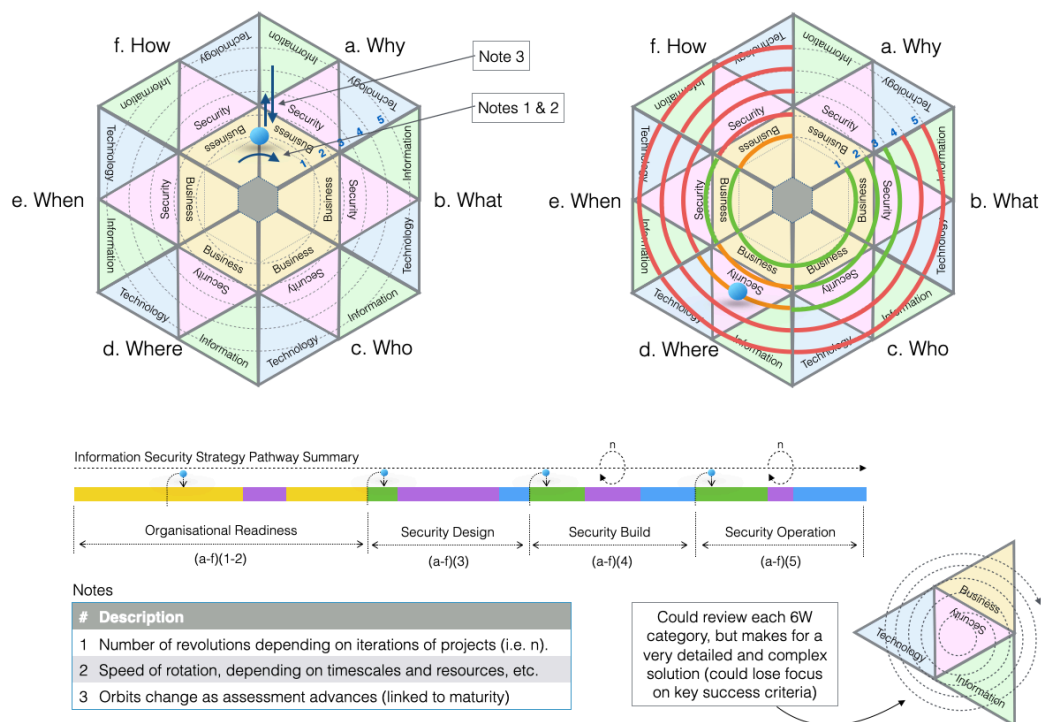


Figure 6.19: Second 6Ws cyclical design concept, separating strategic disciplines

ensure that business perspectives were considered before looking into security issues. Increasing perspective was then given to information and technology, with a corresponding reduction in business, and then security, perspectives. Here, a RAG (Red, Amber, Green) status for portions of a conceptual track are showing which sections of the model have been met. In this concept version the details of each track included many potential checks across the various strategy disciplines (i.e., 18 checks for the outer tracks). This is unlikely to support the design **Goal #9: Quick to conduct assessments**

and would extend the artifact's focus beyond just the key IS issues, thereby missing design **Goal #6: Focus on the key issues that prevent common IS failures.**

There is also insufficient data identified in my root cause analysis for this design and it would therefore over-fit the data available. This approach reflected how the influence of the groups changed with increasing maturity (e.g., business to security to technology), but it was not reflected in the literature, where I found that the relationships between tasks and events do not follow this linear approach. This is especially true for agile projects, and this design would be more suited to traditional waterfall designs. This design characteristic was not taken beyond this concept version.

6.5.3 Discontinuing with the 6Ws categorization

The 6Ws approach is a basic way of information gathering that is used in many industries, but I have found no scientific study that links this concept to enterprise architecture. It helps in the creation of a seemingly logical matrix in some EA frameworks, such as Zachman [184], by arranging the six questions as a vertical axis, with the horizontal axis formed by the multiple layers of an enterprise framework. Whilst all enterprise architectural elements will have to answer one of these questions, my research has shown that structuring architecture in this way may have good style⁵ but it lacks any scientific basis. Other scientific studies of EA frameworks have also failed to identify how EA artifacts could actually be mapped to the cells in this style of framework [97]. My finding also concurs with Kotusev and Kurnia's findings [98] in relation to their *Management fashion theory* (see Table 2.15 for an explanation of this theory).

I decided to use the eight domains for my artifact instead of the 6Ws structure. The use of 6Ws categorization is an attempt to establish consonance with existing EA frameworks, but it does not provide a balanced perspec-

⁵For example, by designing an EA framework that applies these 6Ws questions across every layer as a principle, e.g., Zachman [184]

tive of the key issues identified from my literature review. Further, aligning to established commercial frameworks in general was not science-based and would only assist in implementing a specific commercial architecture framework. My research had shown that there was little evidence that any of the main architecture frameworks (including Zachman and TOGAF) had proven to be successful in business [98].

To demonstrate why the 6Ws categorization does not match my coding of the literature, Figure 6.20 shows the distribution of all 65 nodes across the 6Ws categories. I also show the correlation coefficient value of the node with the highest correlation with failure/success.

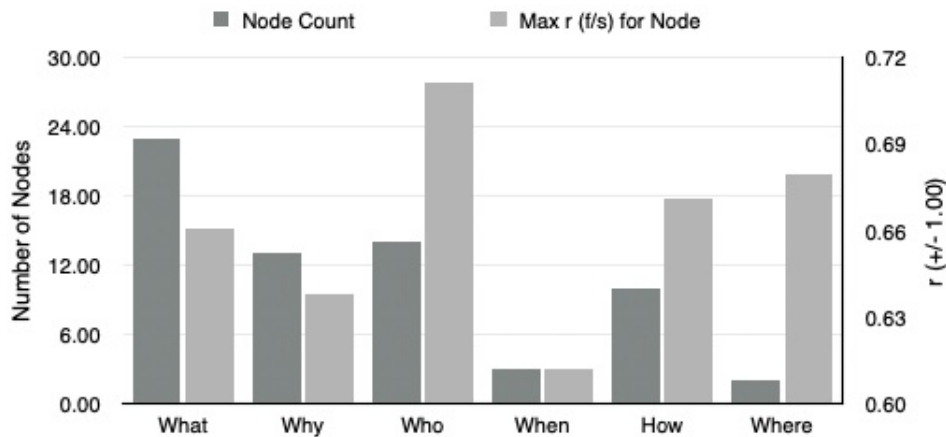


Figure 6.20: Summary of 6Ws category distribution

It is clear from Figure 6.20 that the 6Ws categorization is not providing either the granularity or proportionality over the specific issues that require rapid and continual assessment for IRSM.

For example, the *What* category contains by far the most nodes (23). It could be referring to technology components or company data, for example. The *Who* category covers the next highest number of nodes (14) and covers end user operations, supervisory matters and governance issues, for example. These are all very different attributes and would require a broad comprehension of the context of *Who* for the associated performance markers under the 6Ws categorization.

Using the 6Ws categorization could cause confusion for anyone conducting

a CAESAR8 assessment of a business change proposal. Absolute clarity on the underlying issues is more important than trying to fit the data to a pre-determined design style. The eight domains were identified from the root causes of failures in ISRM identified from the literature and provide a more precise structure for CAESAR8, see Section 5.2.

It was also important to compare how the two schemes (6Ws and 8 domains) address the main fifteenth problems identified in the literature review, so I mapped the fifteen problems to all of the appropriate 6Ws categories. The results are shown in Table 6.6.

Problem #	Why	When	Who	What	Where	How	Total
1			X				1
2			X			X	2
3		X				X	2
4		X	X				2
5			X				1
6	X		X	X		X	4
7	X	X					2
8			X	X			2
9			X	X		X	3
10	X	X				X	3
11	X			X	X		3
12	X	X		X			3
13			X			X	2
14	X	X				X	3
15			X				1
Total	6	6	9	5	1	7	34

Table 6.6: Problems distribution for the 6W questions

My findings are clear to see when displayed in a graph, see Figure 6.21.

The 6W categorizations did cater for every node that I discovered in the literature, but it would not provide a good basis for creating an easy-to-use checklist as it is too abstract. Nor would it provide an easy-to-understand visualization of holistic factors for continually assessing information security risks in lean and agile projects. The 6W questions are too indistinct and

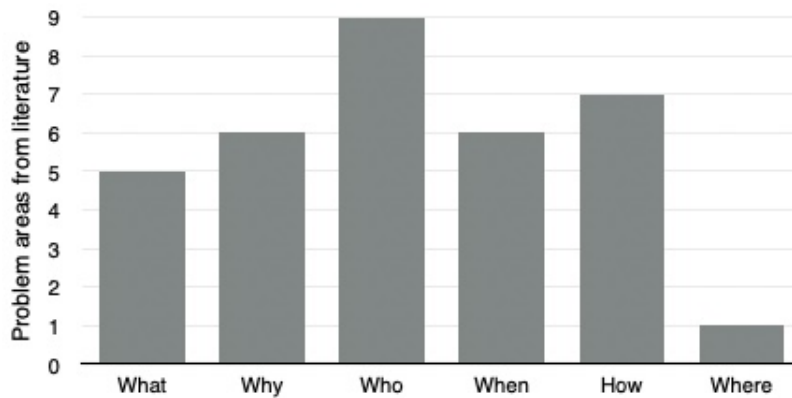


Figure 6.21: Distribution of the 15 problem areas under 6W's

too easy to misinterpret. The cells within this model framework (see Table 2.5 for an example framework based on the 6Ws) do not fit the holistic perspective for the root cause information security risk factors from my analysis.

I repeated the process, but mapping the 15 problem areas across the eight domains. Table 6.7 shows the results.

Problem #	EF	SG	BP	IA	TI	HF	MI	EA	Total
1							X		1
2		X							1
3	X		X	X	X	X		X	6
4							X		1
5	X								1
6		X		X				X	3
7	X		X	X					3
8					X				1
9						X	X		2
10		X	X		X			X	4
11	X			X					2
12	X	X			X			X	4
13		X	X			X	X	X	5
14					X				1
15						X	X		2
Total	5	5	4	4	5	4	5	5	37

Table 6.7: CAESAR8 domain problem distribution

Table 6.7 demonstrates how the problems are addressed across more of these domains than is the case with the 6W’s model. Trying to address these problems in one, or just a few questions under the 6Ws categorization, is not sufficient. This data is shown in graphical form in Figure 6.22, and it shows how evenly these eight domains address the 15 problem areas. The eight domains more accurately reflect how stakeholders should evaluate progress of a project than with the 6Ws categorization. The total number of problem references for the 8 domain model is also greater than with the 6W’s model shown in Table 6.6. This was a count of 37 references compared to 34, so the eight domain model had provided greater reference to the problem areas identified.

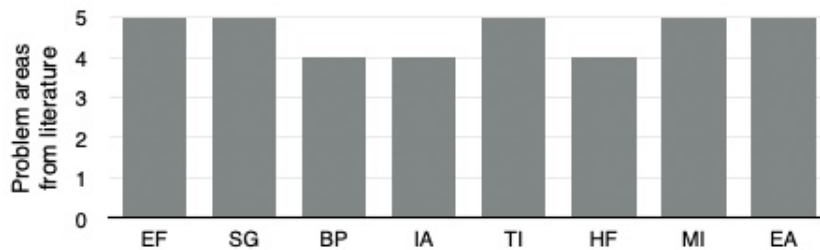


Figure 6.22: Distribution of the 15 problem areas per domain

For certain levels of the architecture (i.e., CAESAR8 maturity levels), a 6W question may surface many times and others not at all. This is certainly the case when addressing the root cause issues that my literature review identified for ISRM, e.g., to address group dynamics or the role of management. For my artifact, the first level/layer would be heavily weighted to *what* questions: what data, what systems, what regulations, etc., as the scope of the change is uncovered. Later levels would be more concerned with *who* and *how*: who will process the data now, how will these people be trained, and so on. The order and structure of the 6W questions is less relevant.

One final example in relation to one of the latest technological advances: cloud computing. In my experience, the decision to store sensitive information outside the corporate network will not be based on a review of company geography and security domain structures, as indicated by the SABSA ap-

proach [154]. Whilst these are indeed important considerations, an agile business decision will be driven by the business need and its urgency to implement an information system to solve a new business problem. In the modern world of cloud services, it will be highly likely that departments will procure cloud-based services from third parties without understanding what vulnerabilities this may create; from privacy issues to business continuity planning. The use of CAESAR8 in these projects will help organizations to collectively understand the true risks associated with these business changes.

The common 6Ws approach was not providing a helpful structure for capturing the most important issues for an agile architecture and I decided to drop the 6Ws approach in favor of the 8 domain model identified in my analysis.

6.5.4 Designing the eight domains into the CAESAR8 model

For the final concept version of CAESAR8, Iteration 2, I configured the CAESAR8 model to use the eight domains identified in my root cause analysis, see Section 5.2. This meant that the objective to **Focus on the key issues that prevent common IS failures** was now being designed into the model's structure.

To satisfy the design objective **Progression must reflect dependencies between deliverables**, I included the second dimension for the eight domains, which was the maturity levels required to progress through the model, see Section 5.4. Figure 6.23 shows the levels from A-E.

This outline design structure also supported the goal to **Allow integration into project management processes or operate stand alone**, as there was a clear process structure (in terms of the eight domains and five levels) that projects could associate with, or link to. Further, **Help to prioritize project work**, is provided by the unique combination of domain and level. The final visualization and metrics ensured that the results are **Easy to interpret and share results at all management levels**.

The final concept version of the model is shown in Figure 6.23.

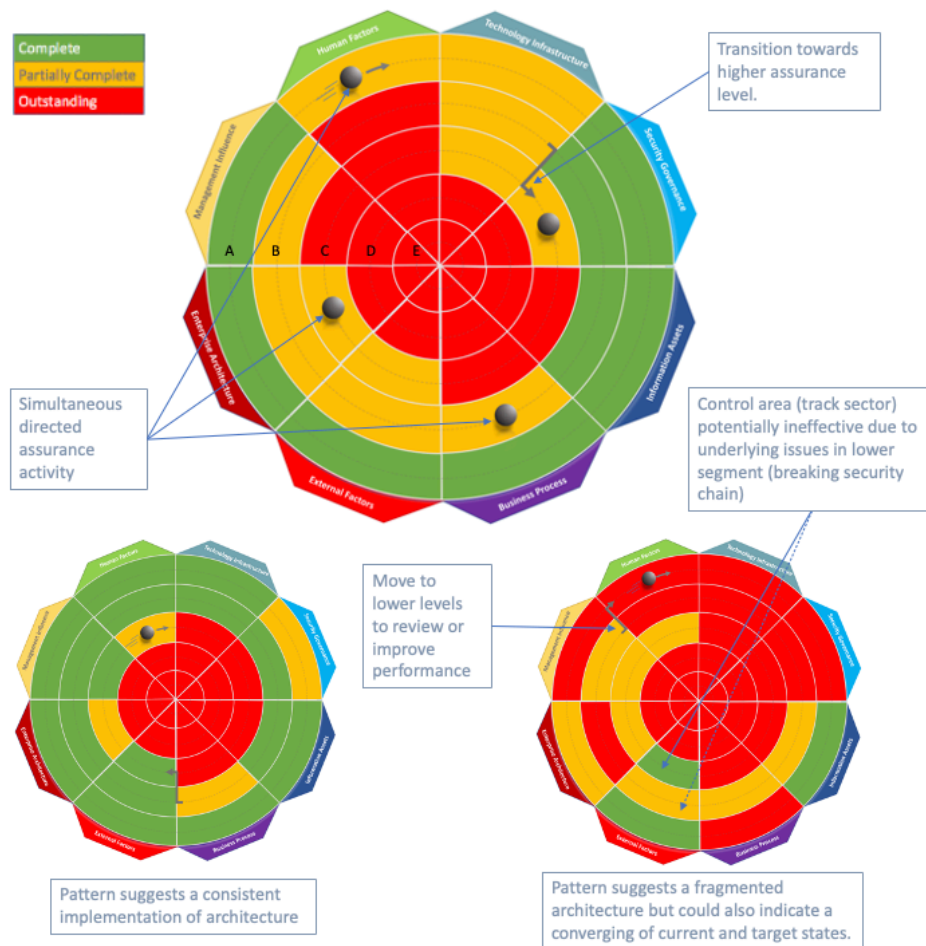


Figure 6.23: The 8 domain CAESAR8 model design

The grey spheres (or *electrons*) depict an original idea where different parts of the assessment could potentially be carried out by different subject matter experts (SMEs). In this concept version, the model is expected to support a single assessment, carried out by multiple SMEs. The grey spheres denote how the multiple parts of the assessment are currently progressing.

6.6 Conclusion of Design and Development

I started this chapter by presenting the five novel design principles of CAESAR8. These principles support an holistic and agile ISRM process in business change projects and were identified through five design and development iterations of the CAESAR8 model.

Next, I described the final iteration of CAESAR8 (iteration 5), which has the ability to capture multiple assessments conducted by knowledgeable project stakeholders and consolidate them into a single result. This shared visualization of the status of ISRM helps to improve the accuracy of ISRM judgments. I provided a description of the multi-stakeholder characteristics that I added to the final design of the CAESAR8 model and provided guidance on how stakeholders should be selected for their cognitive diversity in the context of specific change projects.

The chapter then described earlier design iterations of the CAESAR8 model to show how the design has progressed through the five iterations. The early working prototype versions (APVs - iterations 3 and 4) were described first, followed by a brief description of the earlier concept versions (ACVs - iterations 1 and 2) that helped to shape the key design principles.

I described how the CAESAR8 matrix developed in Chapter 5 allowed the later CAESAR8 prototype models to be demonstrated in operation. For these demonstrations, case studies have been used, both real and synthetic, and have shown that using the CAESAR8 model would have identified all of the information security failings presented in the case studies.

The completed CAESAR8 design principles enabled the development of a CAESAR8 model exemplar, in the form of a cloud-based web app. This web app instantiation was used for the ex post external evaluation of CAESAR8 by industry experts and this evaluation is described in the next chapter.

Chapter 7

Evaluation

This chapter describes the **ex post** evaluation of the artifact, which is DSRP Step 5 in Section 3.2.5. This is the definitive evaluation of the artifact and serves to demonstrate efficacy of the model in relation to its ability to help security teams solve common problems identified for information security risk management (ISRM).

7.1 Methodology

The final iteration of the model was now designed to cater for multiple individual assessments that can be combined to provide an overall evaluation of information security risks for a given business change. For a rigorous evaluation of the model, volunteers conducted *hands-on* reviews of the model's ability to combine multiple assessments.

To support the independent, expert evaluation process, I used the multi-user, web-based instantiation of the model that I described in Section 6.2.2. Using this web app made the assessment and consolidation process easy for the volunteers and it allowed me to centralize and analyze all data created during the evaluation process.

All volunteer web app user IDs were created by me in advance using a random string generator. The IDs were based on a mix of uppercase letters, lowercase letters and numbers.

7.1.1 Two-part evaluation process

The evaluation of CAESAR8 was conducted in two parts with half of the selected industry volunteers completing the evaluation between June and September 2020 and the other half between April and May 2021.

The time interval between part 1 and part 2 allowed for analysis of the results and a review of progress, and part 2 increased the pool of data available for the analysis of results.

The evaluation process was identical for both parts and the results have been combined.

7.1.2 Ethical approval obtained

Before the evaluation process was started and any questionnaires were issued to volunteers, ethical approval was obtained from the University (DMU reference 1920/558).

7.2 Procedure

The CAESAR8 evaluation was performed as a three-step process:

1. A pre-evaluation questionnaire was issued to volunteers to test the problems with IRSM that I had identified in my research. It was also used to confirm the demographics and experience of the volunteers;
2. Volunteers were asked to conduct CAESAR8 assessments for multiple stakeholders¹ for one of their own projects using the web app;
3. A post-evaluation questionnaire was issued to participants to capture their views on how well CAESAR8 helps to address the original problem areas that were identified, and also whether its design goals have been met.

¹The volunteers conducted all of their own assessments but using different perspectives for their own projects, based on their own experiences.

7.2.1 Questionnaires (Pre and Post Eval)

The questionnaires were developed using JISC Online surveys (formerly BOS). This system was licensed by De Montfort University and ensured the security of the data (JISC claims that strict information security standards are followed (ISO27001) and the data is processed in compliance with GDPR). As well as providing all of the questionnaire design features that I required for the evaluation, this system also handled piloting, access control, emailing, piping - used for the distribution of volunteers' unique web app user IDs - and other management functions. This allowed me to chain all 3 phases of the evaluation together. For example, if I did not receive formal consent to the evaluation letter, the questionnaire would be terminated and no user ID issued.

Full transcripts of both questionnaires can be found in Appendix D. The first page of the pre-evaluation questionnaire required all volunteers to sign a formal consent letter covering the research and protection of their personal data. Volunteers could not continue without providing consent. All surveys were kept anonymous.

The design of both questionnaires was 'semi-structured', meaning that there are a set of options provided that respondents are required to select from, but there is also an open-ended option that allows other information to be included. Most questions were based on a 5-level Likert scale [108], which is a psychometric scale for analyzing collective responses. The options were: (1) *Strongly Disagree*, (2) *Disagree*, (3) *Neither*, (4) *Agree*, (5) *Strongly Agree*. Questions also included a free-text response so that any other comments could be captured².

The full questionnaires are provided in Appendix D. The questions are directly related to the problems identified in the literature review and the design goals that I created to address them. Section 4 provides full details of the problems identified and the rationale behind the design goals to address them, including dealing with the underlying issues and incorporating the re-

²This semi-structured design characteristic turned out to be a valuable feature that volunteers used extensively to explain why their scores were given.

quirements of lean principles in the artifact’s design.

7.2.2 Volunteer Training for the web app

After completing the the pre-evaluation questionnaire, volunteers were presented with the web app URL and their unique ID on the final ‘thank you’ screen of the questionnaire.

The web app contained two short training videos and these were presented to volunteers on the landing page of the web app, see Figure F.4, in Appendix F. These videos consisted of: i) a 3-minute video to explain the design of the model³; and ii) a 10-minute visual tutorial of how to use the web app.

I have uploaded the tutorial as an unlisted YouTube video and it is available here: <https://youtu.be/2fLuOi4aC-s>.

These videos ensured that all volunteers received the same level of instruction on the model and app. Full user instructions were also included in the web app as a reference, and the web app also included a default section to allow participants to pre-define their own evaluation data, making the web app easier and quicker to use, as this information was presented to users by default.

The videos received positive praise by volunteers and analysis of the app’s data showed that this enabled volunteers to immediately start using the web app. Offers of additional help and links were made prominent in the web app, but only one minor request was received, and this was to remind the volunteer of their unique ID.

7.3 Assessment criteria

The primary objectives of the evaluation were to check that the original problem areas identified in the literature review are correct (Problem Iden-

³A transcript of this video can be found in Appendix H.

tification, from DSRP Step 1) and had been addressed by CAESAR8. The original design goals for CAESAR8 (Objective of the artifact, from DSRP Step 2) were also checked with the experts to evaluate how effective the key design criteria had been delivered.

The pre-evaluation questionnaire tests the problem hypothesis, by asking experts to rate the original problem identification.

The post-evaluation questionnaire obtains the experts opinion of how successfully the model addresses the original problem areas. In addition, the post-evaluation questionnaire asks experts whether the model had achieved the design goals that were derived from the problem identification. In effect, this process provided a double assessment of how well CAESAR8 is able to help with the problems identified.

It was not made explicitly clear to the volunteers that the same problem areas were being examined. The wording of the problems between pre and post evaluation questionnaires was altered as described in the next section. Volunteers were also asked to provide their findings about CAESAR8's multi-stakeholder capability.

Finally, volunteers were asked to provide some details of their own experience in relation to information security.

7.3.1 Assessing the Problem Identification

The common areas are summarized in Section 4.1.1, and are shown here in Table 7.1. The original wording was included in the pre-evaluation questionnaire but the wording was revised slightly to test for potential benefits of CAESAR8 in the post-evaluation questionnaire. Both versions are included together in Table 7.1. The categorization was included in the pre-evaluation questionnaire only, and provided volunteers with more information about the context of the problems.

#	Problem Pre-evaluation questionnaire	Benefit Post-evaluation questionnaire
Governance Problems		
1	Stakeholders not directly engaging with projects	Ensuring all stakeholders maintain active involvement in projects
2	Lack of collaboration across separate teams	Supporting collaboration across separate teams
3	Limited understanding of the wider effects of changes	Maintaining an holistic perspective when agreeing changes
4	Executive not formally understanding project risks	Obtaining senior management acceptance of project issues and risks
Solution Design Problems		
5	Legal compliance reviews not completed for all changes	Completing legal compliance reviews for all changes
6	Security risk management not expressed in a business context	Security risk management is understood in a business context
7	Insufficient rigor applied when working with third parties	Applying rigor when working with third parties
8	Agreed security controls are sometimes omitted	Ensuring that agreed security controls are fully implemented
9	Lack of monitoring of security controls	Ensuring security controls will be monitored
10	Project impact on current business processes not fully considered	Full understanding of how a new system impacts on current business processes
11	Lack of clarity over information storage and sharing	Clarity over information storage and sharing
12	Ad hoc deployment of new technology	Ensuring that new technology is implemented in a controlled manner
13	Not understanding the effect of a new system on all personnel	Understanding how a new system impacts all effected personnel
14	Testing is not completed adequately	Ensuring that testing has completed adequately
15	Management unwilling or unable to monitor compliance	Ensuring that management will monitor system performance

Table 7.1: Evaluating the problem areas between pre and post evaluation questionnaires

In addition to the problems identified in the literature, the implementation of CAESAR8 also needs to help address the nine underlying issues.

These were described in Section 4.1.2.

As can be seen from Appendix D, the questionnaire was semi-structured and also asked experts to specify any other security issues that implementation of the model needs to accommodate.

7.3.2 Assessing the Design Goals

The *post-evaluation* questionnaire was used to ask experts if they agreed that the designed artifact would address the problems that were identified at the start of my research. In addition, volunteers were asked to rate how well CAESAR8 had met its design goals.

The order and the wording of the goals were changed to relate to the specific CAESAR8 characteristics that had been developed from the design goals. This prevented the more abstract and potentially pre-loaded questions of the original design goals.

Eleven design goals were tested in the evaluation are provided below (Table 7.2), mapping against the original Design Goals described in Section 4.2. (Note: The first design goal described the intrinsic design of the artifact and was thus removed from the final set of questions.)

The second column of numbers (vQ) provides a cross-reference to the order of the goals as they appeared in the post-evaluation questionnaire.

For the purposes of the design and development process, the Goals were grouped by their specific area of focus, i.e the overall design, usability and governance.

#	vQ	Design Goals	Evaluation Questions
Design focus			
1	0	Base on a non-linear design that encourages continuous re-assessment of changes	<i>(No separate evaluation question, as intrinsic to the design)</i>
2	6	Progression must reflect dependencies between deliverables	The levels (1-5) were meaningful
3	8	Allow integration into project management processes or operate stand-alone	It was easy to integrate CAESAR8 with existing DevOps and Project processes
4	9	Fully embrace Agile values	CAESAR8 supports integration with Agile working practices
5	11	Encourage just-in-time updating of EA artifacts	CAESAR8 will help to maintain essential architecture documentation
6	1	Focus on the key issues that prevent common IS failures	The 40 questions covered some key issues to determine success
Usability focus			
7	2	Provides an easy to understand, repeatable review of the most critical issues	It was easy to conduct assessments
8	3	Easy to complete assessments	The 40 questions were easy to understand
9	4	Quick to conduct assessments	Conducting assessments was a quick process
Governance Focus			
10	10	Help to prioritize project work	CAESAR8 assists with the prioritization of work
11	5	Ensure all business departments' perspectives are represented	It was valuable to include multiple stakeholders when conducting assessments
12	7	Easy to interpret and share results at all management levels	It was easy to share results with all colleagues and management

Table 7.2: Evaluating the Design Goals

Finally, Iteration 5 had highlighted the significant and novel feature of combining the individual assessments of multiple stakeholders, thus *ensuring all business departments' perspectives are represented (Goal # 11)*. Therefore, additional criteria for these unique characteristics were added to the post-evaluation questionnaire:

1. Additional stakeholders could be from other, non-security roles?
2. The CAESAR8 assessments provided relevant questions for other stakeholders?
3. The stakeholders could identify performance markers that were relevant to them?
4. Stakeholders can provide just the responses where they have knowledge/responsibility?
5. It was easy to combine separate assessments and collaborate on the results?

A copy of the complete pre- and post-evaluation questionnaires are provided in Appendix D, which shows the additional criteria captured for qualitative assessment and participant characteristics.

7.4 Participant characteristics

As the model is specifically intended to obtain the views of diverse stakeholders, the pool of experts included a diverse group of experienced stakeholders involved in cyber security projects. I refer to the volunteers as experts in the results. A summary of the experts that took part in the evaluation is included in Table 7.3.

#	Type	Role	Identifier
Part 1 evaluation			
1	Security	Information Security Professional	S1
2	Security	Information Security Professional	S2
3	Security	Information Security Professional	S3
4	Business	Senior Project Manager	B1
5	Business	Business and Operations Manager	B2
6	Technical	Software Engineer and Auditor	T1
7	Technical	Software Engineer	T2
Part 2 evaluation			
8	Security	Information Security Professional	S4
9	Security	Information Security Professional	S5
10	Business	Business Cyber Lead	B3
11	Technical	IT Change Manager	T3
12	Business	Program Manager	B4
13	Security	Information Security Professional	S6
14	Security	Information Security Professional	S7

Table 7.3: Evaluation volunteers for part 1 and part 2

All experts had more than 10 years of experience in their respective fields, and all had experience on technical cyber-security related projects. I also grouped the experts into one of 3 *types*, based on their primary roles: Security, Business and Technical. Although half of the experts invited to take part were experienced information security professionals, I deliberately chose to include experts from other diverse backgrounds to test the stakeholder diversity benefits of CAESAR8. CAESAR8 has been designed to bring the benefits of more holistic risk assessments to a wider cross section of a typical project community.

By analyzing the data stored by the web app, I could tell that some volunteers had spent over an hour just working on individual assessments in the web app. This does not include the time taken to complete the two questionnaires, watch the training videos and configure default options, including their stakeholder selections, and view the results. Analysis of the web app data showed that participants sometimes conducted their assessments over many hours, days, or even weeks. Therefore, I was asking for a substantial commitment from volunteers and these volunteers needed to be impartial and

experienced. The evaluation needed to be kept small in size but conducted rigorously.

Fourteen volunteers started the evaluation process and completed the pre-evaluation questionnaire, but three volunteers did not complete the evaluation. Therefore, analysis of the post-evaluation questionnaire is based on eleven responses.

I asked experts to describe the frequency for which they are engaged in the security activities shown in Figure 7.1. The figure provides a guide of the approximate number of days per year (based on the frequency provided) that a participant is engaged in the specific activity using a 48 week working year. These are approximations only and serve to provide an understanding of the relative difference between time spent on these activities for a diverse group of experts with IS responsibilities (half of the volunteers were IS professionals).

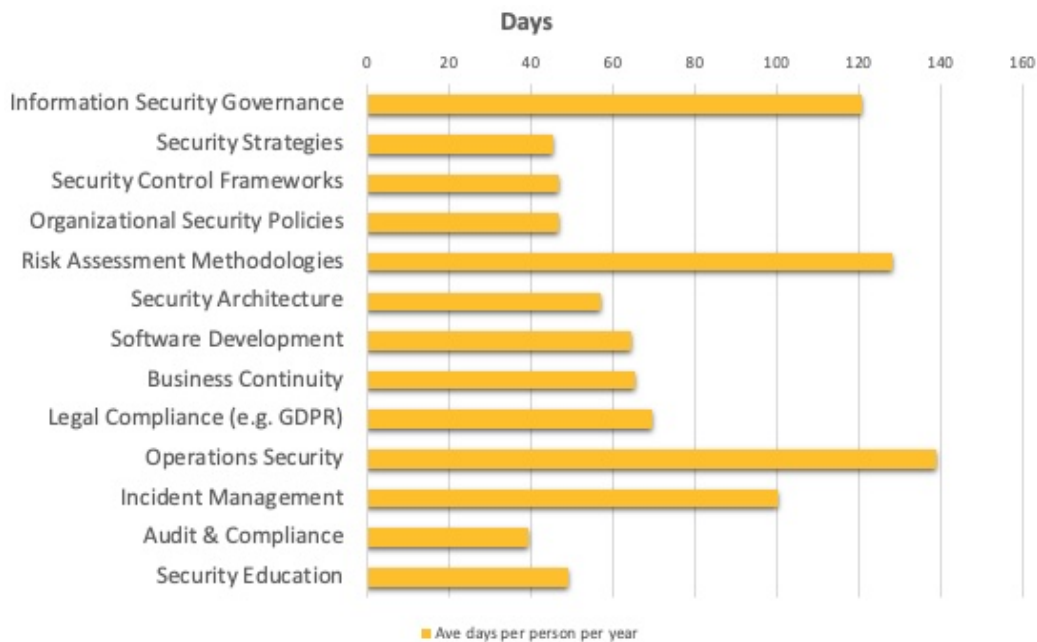


Figure 7.1: Average annual activity for professionals

These key observations are relevant for my study are:

- Most experts were heavily involved in routine security operations, incident management and governance issues.

- Time spent on security strategy and control framework is low, as is audit and compliance activity. This indicates the hands-on nature of the experts.
- Time spent on legal compliance was relatively high, which might explain why this is perceived as less of a problem than expected when assessed later on in the study (see Figure 7.4).
- Time spent conducting risk management was high. This is a key target area for the CAESAR8 model.
- Despite risk assessment activity being high, security architecture and strategy work is relatively low.
- Experts involved in the study had experience across a broad range of security activities.

7.5 Results of Evaluation

This section provides my analysis of the results but the coded raw responses to the questionnaires are included in Appendix D, Section D.2.

The experts' opinions of the fifteen problem areas identified in the literature review are discussed first, followed by a review of each design goal.

The results are often expressed as an average for all experts collectively, or for their type groups. No questionnaires have been excluded from the results presented.

Many comments were volunteered by the experts in relation to how the CAESAR8 model is focusing on key issues. I have included relevant comments in my analysis, but here are a couple of general examples:

“The tool allows an easy overarching view providing areas of a project or business change that require enhanced attention and effort in order to achieve the desired business assurance.” (S3)

“[CAESAR8] helps to corral key areas of concern. Once I had used the tool I can see how it is useful in providing a dashboard to highlight areas of concern.” (S1)

7.5.1 The 15 problems areas

CAESAR8 has been designed to resolve fifteen over-arching problem areas for ISRM (Problem Identification, from DSRP Step 1). Therefore, I wanted to start my evaluation by asking experts if this had been achieved.

To do this, I obtained ratings for these 15 problem areas in the pre-evaluation questionnaire, so that I could determine how closely the experts agreed that these problems exist in their work environments. I then included the same 15 problems areas again in my post-evaluation questionnaire, but this time by asking to what extent CAESAR8 is helping to address them. The wording of the questions as they appeared in the two questionnaires differed slightly and is shown in Table 7.1 for comparison.

When analyzing how CAESAR8 performed across the categories of problems (Governance or Solution Design), there was a very even split, as can be seen in Figure 7.2. For each category, a y-axis ≥ 4.0 means that, on average, volunteers agreed with the problems that I identified in the literature existed for information security projects, or agreed that CAESAR8 will provide a solution to these problems. All four of these categories were greater than 4.0. This confirms that CAESAR8 should provide a closely matched solution to the 15 problems areas identified in the analysis and should benefit agile projects from both a governance and a more technical design perspective.

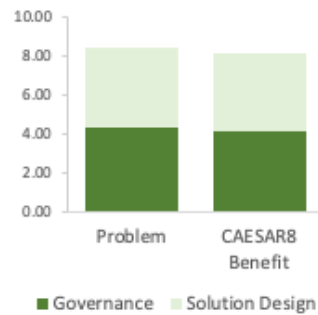


Figure 7.2: Problems by category

Figure 7.3 shows a plot of all fifteen problem areas together with their corresponding CAESAR8 benefits, where each dot indicates the average response for a problem area/benefit combination.

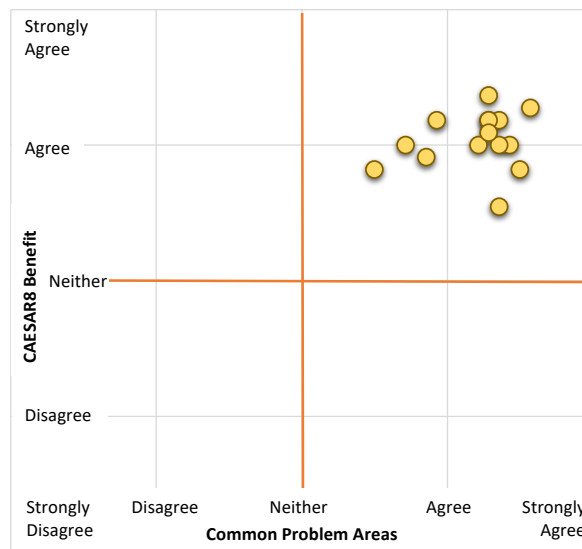


Figure 7.3: Common problems matched to CAESAR8 benefits

All fifteen problems are positioned in the upper-right quadrant, indicating that the experts confirmed that CAESAR8 was helping to improve known information security problems in projects.

Figure 7.4 shows how this data relates to the individual problem areas.

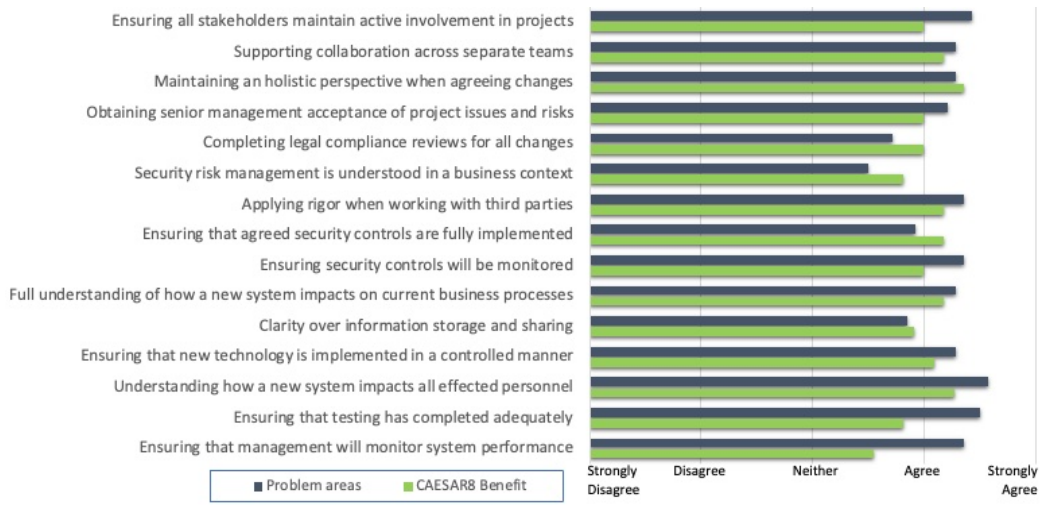


Figure 7.4: CAESAR8 Benefits to address the 15 common problems

A key and unique contribution of CAESAR8 is its ability to capture the broad perspectives of all those stakeholders genuinely involved in a change project. In particular, five of the problem areas relate to stakeholders. Just these five problems are examined in Figure 7.5, where it is easier to see that the experts concur with the problems identified and confirm how CAESAR8 can help in addressing them.

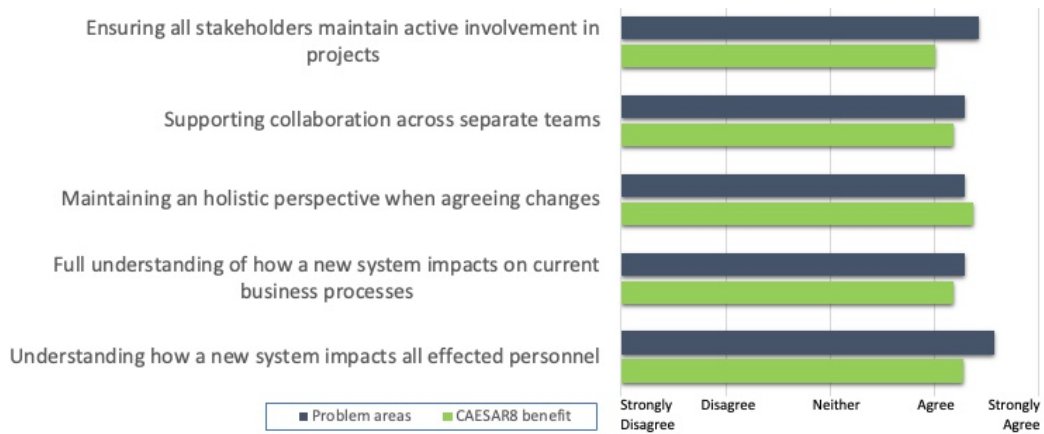


Figure 7.5: CAESAR8 Benefits to address the 5 stakeholder-related problems

Experts commented that the value of the model will depend on how it is operated and supported within business, and this was reflected in their

individual assessment. An experienced Change Manager who took part in the evaluation, offered the following comment:

“The process of checking must be adopted by all levels. Management and senior engineers, very often, for expediency, determine that documented processes they have signed up to can be side stepped in order to fulfill a timeline. This always causes problems long term when short termism is employed.”
(T3)

Another comment about the problems of maintaining governance was made by an information security professional:

“Shadow IT to circumvent the need to involve InfoSec..” (S6)

The comments have indicated that if CAESAR8 is embraced by the whole change program and fully supported at all levels, the benefits will be even higher than the scores that experts have given in the evaluation. The model has been designed with these problems in mind. Proper implementation of the model will be key to CAESAR8’s ability to deliver benefits to an agile change project (Section 6.3 discussed the implementation of CAESAR8).

For two problem areas, agreement with CAESAR8 providing a benefit was greater than half a point (> 0.5) lower than agreement with the problem area (on the five-point Likert scale used): *management monitoring of system performance* and *ensuring completion of adequate testing*.

Whilst CAESAR8 encourages adequate checks for monitoring of system performance, actually delivering this requirement will still need to be enforced by management to ensure that it actually happens (CAESAR8 actually scored 0.81 points lower than the problem score). However, CAESAR8 will help by providing a number of checks across the maturity levels (e.g., checking for responsibility, a documented procedure, and the means to carry it out).

Satisfactory testing is a problem recognized by all groups (although CAE-

SAR8 scored 0.68 points lower than the problem score), and my earlier research has shown that thorough testing of security controls is important to fully understand potential failure modes. However, tight project deadlines can encourage skipping of vital elements of the testing programs. While all experts agreed that CAESAR8 would help to ensure that testing is completed adequately (see Figure 7.3), I wanted to understand whether the model could be improved to address this issue, as all experts agreed that it was a problem with 50% strongly agreeing. When I examined the related performance marker, TI4, I noted that this marker only requires a check for a plan; it does not check that the plan was put into operation. Therefore, I decided that I needed to make change to this performance marker. I describe all of the changes to performance markers in the discussion at the end of the results.

For the legal compliance problem area, the experts confirmed that CAESAR8 is providing a solution to this problem, but the actual problem was scored as less relevant than I expected. Both my experience and the literature review have highlighted how legal compliance is a significant issue [31] and particularly for smaller organizations who may need to outsource information processing [33]. When I reviewed how experts had scored and commented on the corresponding performance marker (EF1), I discovered that there had been *Yes* and *No* responses, and also a *Trust* response - the latter accompanied with the comment that this responsibility is “*dispersed across various organizational groups*” (*expert S2*). This is exactly the type of response that I was envisioning, and it underlines the significance of including all relevant stakeholders. Therefore, the EF1 performance marker remains unchanged.

7.5.2 The diversity and inclusivity of CAESAR8 assessments

Having a diverse group of individuals independently conducting assessments requires a common frame of reference. I created this frame of reference by providing a common checklist for all stakeholders in the form of the 40

performance markers. This checklist is not intended to standardize responses, but to provide a common, cognitive focus for all stakeholders involved in the assessment. Checklists are not “how-to guides” [58], but are quick and simple tools aimed to buttress the skills of expert professionals. My analysis of 15 common problem areas for information security in agile projects has been agreed by the experts, who have then confirmed that CAESAR8 will help to address them. However, it is interesting to note that not all experts regard these problems in the same way. Figure 7.6 shows how different groups of experts rated the problems that I presented in the analysis.



Figure 7.6: Expert category split on 15 common problem areas as they were presented in the pre-evaluation questionnaire

These differences among experts are to be expected and makes a strong argument for integrating diverse opinions into the assessment of security risk, as we cannot measure what we personally do not know. It may not be new

information that is needed, but a new perspective (i.e., the knowledge) on the severity of the residual risk before a change can progress with confidence. This is a key concept that the CAESAR8 model is intended to address. A notable difference is the disagreement by security experts that security risk assessments are not always understood in a business context. Conversely, the business and technical experts agree that this is indeed a problem area. This difference is unsurprising, as security professionals are often required to conduct the security risk assessments. However, the simple stratification methods (e.g., 2D matrix) that are often used in IT security have been shown to have serious flaws in their analysis of risk [6] and are often based on the self-assessments of individuals. To achieve a better forecast, CAESAR8 models the key components of the system (i.e., the enterprise domains), rather than the behavior that we are predicting ourselves [77].

7.5.3 Underlying Issues

I asked the experts to comment on the underlying project issues that can be a hindrance to information security, including time pressures, budgetary constraints, high workloads, volume of changes, and prioritization (these are the *underlying issues* described in Section 4.1.2 and have been key considerations for my research). The results are shown in Figure 7.7.

When analyzing the individual responses that all experts gave for all eight issues, 94% of experts were in agreement that these underlying issues existed for information security projects. Of greatest concern are the change project budget and time constraints, along with the volume of changes that projects can undergo. High workloads and clarity over prioritization can also be a challenge for the whole project team.

Awareness of time-related pressures was particularly important when designing the model, so that its design is heavily focused on delivering maximum benefit with minimum additional input. This allows the model to provide continuous, repeated reviews by all stakeholders working in a rapidly changing agile program. The wider effect of rapidly changing iterations of business change projects needs to be quickly assessed and any issues identified and



Figure 7.7: Experts' views on the underlying (business) issues

addressed. For example, the following associated comment was provided by a business expert:

“Security process and tools slow down deployment and make it harder for project to complete within time budget . Security seen as a barrier to progress rather than an enabler.” (B4)

Whilst experts had the ability to propose other challenges that they have faced whilst working in information security projects in business environments, their comments were a reinforcement of these problem areas: e.g.:

“Those designing the solution putting their efforts and focus on the wrong areas due to lack of engagement” (S6).

“Nothing to add to the list. Despite many examples of issues occurring there is generally a focus on project (commercial) achievement, with considerations of IS remaining the responsibility of the IS profs. As such there is a

clear fault/blame line irrespective of how well the IS team is funded/staffed and hence no matter how severe the consequence someone can be the scape-goat.” (B3)

The lack of adherence to security operating procedures was a recognized issue, and is reflected in the model by an emphasis on the important role of middle management, represented by the Management Influence (MI) domain. Most of the experts agreed that recruiting skilled security staff was not a major problem, except recruiting more technical security staff.

7.5.4 Analysis of the Design Goals

Following my evaluation of the problem areas, I needed to check that the design goals for CAESAR8 had been achieved, as this would confirm its utility as a practical solution for businesses. As described at the beginning of this chapter, the post-evaluation questionnaire used wording for the design goals that specifically related to how CAESAR8 addressed the goals. Table 7.1 provides a mapping between the original goals and the evaluation criteria. However, the results described in this section are ordered as per the original goal reference numbers.

The results are shown in a box-and-whisker plot in Figure 7.8, which shows that there was overall agreement that the new CAESAR8 model achieved all eleven elements of the original design goals.

The box plot splits the results into quartiles, with the interquartile range forming the box. The plot inside the box is the median, and whiskers indicate the variability outside the upper and lower quartiles. Outliers are shown as separate points.

The remainder of this section includes a detailed analysis for each of the eleven design goals.

Design Goal #1 - Base the model on a non-linear design that supports and encourages continual reassessments of ongoing changes

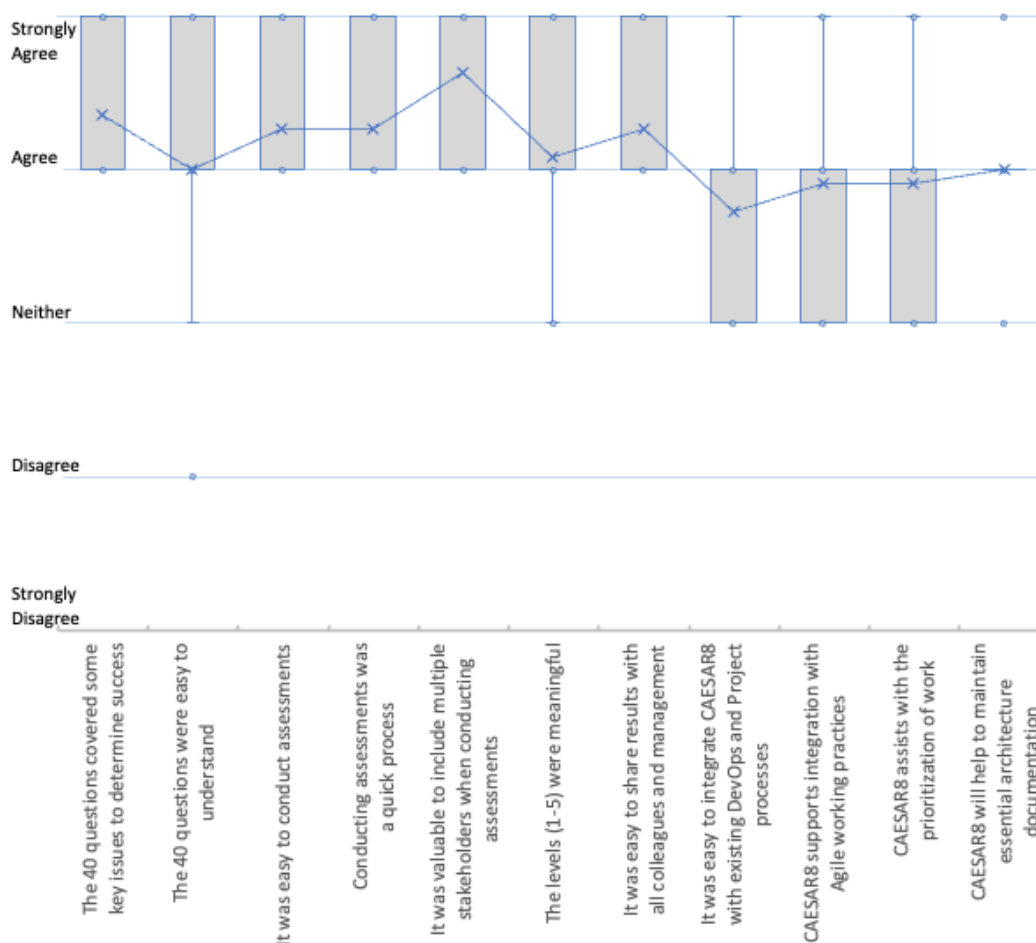


Figure 7.8: Box-and-whisker for the experts' assessment of the 11 Design Goals

to projects. This design goal was intrinsic to the design of the artifact and is a statement of fact. Therefore, it was not included in the evaluation of CAESAR8, although results and comments for other design goals confirmed that this objective had been achieved.

Design Goal #2 - Progression through the model should reflect the dependency between security activities. The dependency is captured by the CAESAR8 levels, e.g., the CAESAR8 Checklist asks if the stakeholder has identified all IT systems that are effected by the change in level 1, before

examining what changes are being made to IT in level 2.

I asked experts if the CAESAR8 levels were meaningful, and this was a strongly supported view with 82% of experts agreeing. An example comment:

“[The model] provides visual and documented evidence of what the status of the change management is.” (B2).

Design Goal #3 - It must be possible to integrate the model within existing project processes. I asked experts specifically about integration within DevOps environments. Referring to the supporting comments when analyzing responses confirms that this question requires knowledge of DevOps. For example, one expert commented:

“I could not answer whether CAESAR8 was easy to integrate with DevOps and project processes.” (T3)

This expert gave a *neither* response. Overall, 64% of experts agreed that this design goal had been met. However, regardless of a stakeholder’s knowledge in this area, they will indirectly contribute to the assessment of development risks, e.g.:

“A really strong concept and definitely a useful way of evaluating security risk.” (T2)

Design Goal #4 - The model must support integration with agile working practices. Overall, 73% of experts were in agreement that CAESAR8 achieves this goal, with the remainder selecting “neither”. Analysis of the comments confirmed a similar situation to goal #3 regarding DevOps, in that not all experts were familiar with agile working practices, so could not answer. In anticipation of this, I had provided some basic information on how CAESAR8 might support agile working environments in my video tutorial. My reasoning for doing this was to show how CAESAR8 was not

designed to work with any specific methodologies that experts may already be familiar with, but can integrate at a fairly high-level with reviews of small project iterations. As one expert commented:

“The ease of use would assist in continued assessment.” (S4)

The experts’ score of this goal confirms the findings in my literature review, which is that the agile concept is often a fluid, hybrid process for many organizations in non-software industries. The model should support agile and lean concepts (by providing agile ISRM approaches) but not become tied to any particular methodology.

Design Goal #5- The model must support the creation of architecture documentation, where required. There were 82% of experts that agreed that this objective had been achieved, with 22% of those in *strong* agreement.

Many of the checks that are relevant for achieving this goal are from Enterprise Architecture domain (EA), and some of the wording within this domain will be familiar to architects, security experts and technical team members. This is similar to the findings for Goal #7 which related to how easy the performance markers are to understand. As was the case with Level 5 performance markers, it may sometimes be acceptable to exclude this domain from quick CAESAR8 assessments that require little or no updating of EA. However, the domain allows stakeholders to describe how the documentation for EA is developing from their perspective and could be important for reducing information security risks.

Design Goal #6 - The model must focus on the key issues that help determine the success of information security in business change projects. This was the first goal that I assessed in the post-evaluation questionnaire, and I asked the experts to rate how well the 40 questions that I devised for the performance markers were capturing the key issues that determine success. As can be seen from Figure 7.8, all experts agreed that I

had achieved this design goal and 36% were in strong agreement.

Levels 3 and 4 of CAESAR8 deal with the security impact and security strategies, but a sequential review of all levels of the model is required to ensure that the results are reliable at these higher levels.

Design Goal #7 - It must be an easy process to conduct assessments using the model. All experts rated this goal as either Agree or Strongly Agree. Everyone was able to start using the model immediately, and no issues or questions were raised during the study. An example comment from a business expert:

“Very easy to navigate the model” (B2).

Design Goal #8 - The checklist must be clear and easy for all stakeholders to understand. 82% of experts agreed that the 40 performance markers (the checklist) were easy to understand. Some comments supported this view:

“The model is a very powerful one, with questions that are easy to understand and apply.” (T1)

However, one security expert warned that some stakeholders may struggle with some of the terminology. This was confirmed in an assessment by a project manager (identified by the low outlier point in Figure 7.8), who advised that guidance was needed at Level 5:

“As a PM, I would need some explanatory notes, particularly on level 5.”

CAESAR8 level 5 refers to optimization, and it is fair to assume that Level 5 assessments require confirmation with a security expert. This can be achieved through CAESAR8 using the *Trust* option. Level 4 should be regarded as the minimum safe level for a business change project to be implemented.

Design Goal #9 - Conducting assessments must be a quick process.

The results were identical to Goal #3, with all experts in relatively strong agreement. One expert commented that:

“The questionnaire [CAESAR8 assessment] was able to be populated quickly and yet provided holistic coverage. The tool provides a framework to enable project governance and point towards areas that require greater effort or scrutiny. The product, in my view, would be a positive mechanism to organizations.” (S3)

Additional information for the usability design goals (goals #7 to #9 are included in the discussion section of the results (Section 7.5.5).

Design Goal #10 - The model must assist with the prioritization of work.

There was positive agreement that this objective had been met by the model, with 73% agreeing and 25% of those *strongly* in agreement. A subtle feature of CAESAR8 that assists with prioritization is how stakeholders can specify that they are trusting another stakeholder to meet a specific requirement. This allows them to refocus their attention on other priorities, whilst alerting the other stakeholders that they may need to reassess their own priorities and ensure that this work is not missed. This will assist projects to identify where there are gaps that need to be addressed before progress can be made for the project as a whole.

Although I made no specific reference to the model’s *Trust* response option in the questionnaires, multiple experts considered this to be a novel feature of the model’s design when obtaining the views of multiple stakeholders, e.g.:

“This model makes those gaps and those areas of ‘assumed trust’ immediately clear. This is something that is enormously powerful” (T1)

“Identifying where one stakeholder is trusting another is a strong feature.”
(S2)

In fact, Figure 7.9 shows the answers that volunteers selected for performance markers throughout the testing of the web app during the evaluation. It can be seen that the *Trust* option was used fairly extensively in their tests (13%), and most performance markers were changed from their default “*unknown*” values (only 1% remained as *unknown*) to a specific answer.

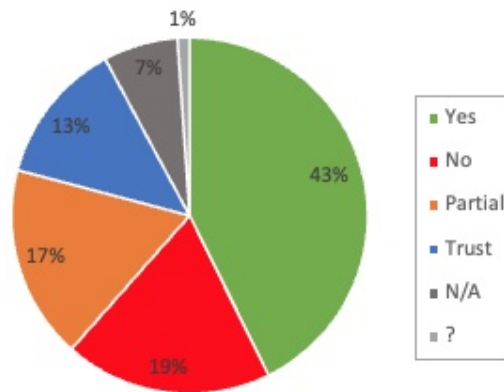


Figure 7.9: Answers that experts gave to the performance markers

Design Goal #11 - Multiple assessments from stakeholders across the organization are required to ensure that information security solutions are correctly aligned with the business. As can be seen from Figure 7.8, this is the model’s strongest feature, with all experts agreeing, and 64% *strongly* agreeing, that this is a benefit of CAESAR8.

The modal average for the total number of assessments that each expert conducted during the evaluation (i.e., separate stakeholder assessments) was three.

Many comments were made by the experts, e.g.:

“[CAESAR8 is] a very powerful model, which has the potential to allow all parts of an organization to be involved in the assessment and ongoing monitoring of cyber security, with significant benefits to the organization.”
(T1)

“I really like the results page and how the different stakeholders results can be overlaid to produce an overall picture.” (B1)

“This is a great model to ensure the ‘buy in’ from all stakeholders..” (B2)

Before seeing the model, all experts agreed that there is a problem ensuring that stakeholders maintain active involvement in projects and 43% of those strongly agreed. It is particularly significant, therefore, that this is regarded as the strongest benefit of the CAESAR8 model, as is shown in Figure 7.5.

In the post-evaluation questionnaire, I specifically asked the experts for their opinions on the benefits of obtaining multiple stakeholder perspectives. The results are shown in Figure 7.10.



Figure 7.10: Stakeholder involvement-related question responses

Overall, 82% of responses agreed that CAESAR8 supports diverse stakeholder involvement, with the strongest being the characteristic of supporting non-security roles. This is important for the success of the CAESAR8 model, since it is reliant on diverse stakeholder involvement.

The error bars shown in Figure 7.10 are based on the standard deviation of the results that the experts gave for each question. They particularly show how the characteristic of “*The stakeholders could identify performance markers that were relevant to them*” was adversely affected by one *disagree* value and one *neither* value. No comments about these two values were provided but all other experts *agreed* or *strongly agreed* with this characteristic. As

can be seen from Table D.9 in Appendix D.2.1, the low responses were both from security experts, rather than the non-security roles.

The error bars also show that the range of uncertainty from the mean values all still lie within the *agree* columns. Therefore, apart from Level 5 of CAESAR8, which deals with optimization, I conclude that CAESAR8 is ideally suited to non-security stakeholders.

Design Goal #12 - It must be easy to share the overall results of assessments for business change projects with all colleagues and management. All experts agreed that this design goal had been achieved with CAESAR8. This was also supported by many comments, e.g.,:

“I feel the model would be really useful for Project Managers. Information security and management information is a complex but critical part of all projects and so often, the Project Manager has to find the answers themselves whilst not having the relevant knowledge. This model provides concrete foundations for the PM to build on and also provides credibility and supports the PM in engaging with all stakeholders and allowing these conversations to take place.” (B1)

7.5.5 The efficiency of CAESAR8 assessments

This section analyzes the data stored by the web app for the purpose of testing the performance of the CAESAR8 usability design goals #7 to #9. The web app recorded time-stamps for each answer that experts gave for the performance markers within their assessments. I used these time-stamps to evaluate the efficiency of the assessment in more detail. I computed the differences between time-stamps which indicates how long experts took to interpret the questions and provide responses.

The results of 449 performance marker assessments are shown in Figure 7.11, which is a box-and-whisker plot showing how many seconds elapsed between questions.

This box plot splits the data for each performance marker into quartiles.

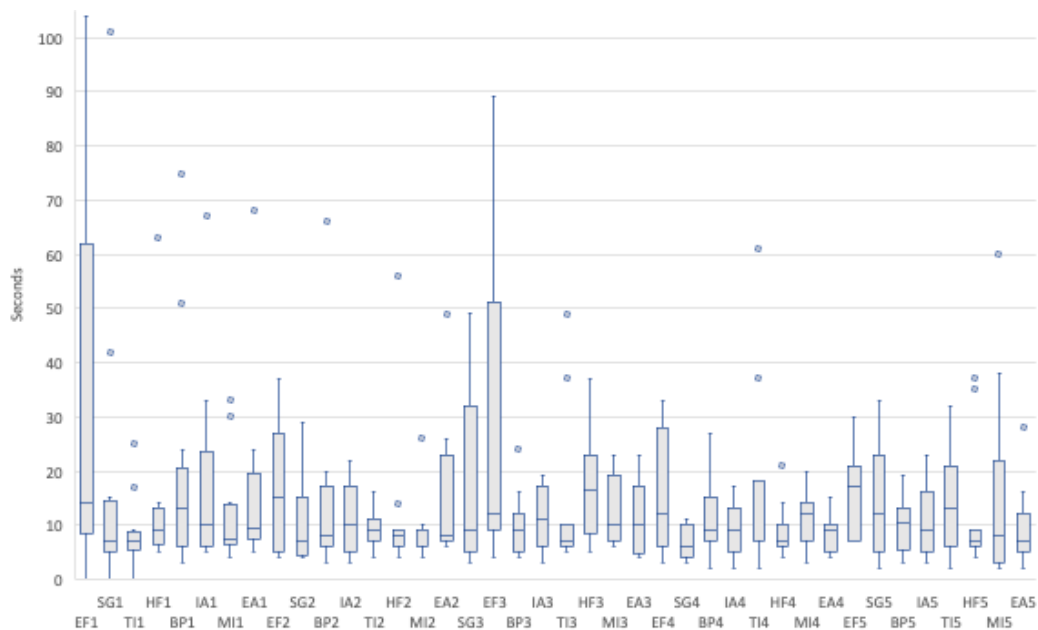


Figure 7.11: Box-and-whisker for user time-taken per performance marker in part 1 of the evaluation

The dividing line in the box is the median, and whiskers indicate the variability outside the upper and lower quartiles. The additional points shown are outlier values, for example, where an expert may have taken a break from the assessment.

The order of performance markers in the web app assessment page is the same as they appear in the diagram. This explains why EF1 has an extended upper percentile and upper whisker, as some experts opened the assessment page and then delayed starting their assessment; most probably examining the page. However, the median for EF1 is still relatively low. The small lower quartiles and larger upper quartiles indicate that experts were regularly taking time to understand and respond to each question. It can be seen that the median is approximately 10 seconds per performance marker, which equates to 6 to 8 minutes to complete the whole assessment. EF3 has a high 75% quartile, but its median is consistent with that of other performance markers. Of more concern are EF2 and HF3, which have higher median values along

with high interquartile ranges. This indicated that a review of the wording was required for these performance markers.

Using this data, I could also identify that the average time that a volunteer spent in testing the CAESAR8 model using the web app instantiation was 26 minutes. Note that this is only the time taken to conduct actual assessments. It does not include time watching the training videos and setting up stakeholders, etc. The longer that a user spent testing the model, the higher their benefit score tended to be. There was a notable correlation between a volunteer's average CAESAR8 benefit score and the time they spent using the web app. I calculated this to be $r=0.49$ for the entire evaluation, but $r=0.81$ for Part 1 alone. Part 2 volunteers only spent 34% of the total time that Part 1 volunteers spent using the app. One expert in Part 2 of the evaluation commented:

“Probably would have needed more practice on combining and presenting assessments to get the most from it.” (B4)

B4 only spent 8 minutes working on specific assessment responses. Note that this is not the elapsed time working on the evaluation, which would have been considerably longer. For example, B4's time spent on the post-evaluation questionnaire alone was double this time (15 minutes).

Another important factor to consider in the efficiency of CAESAR8 assessments is the relatively quick speed at which separate stakeholders can conduct assessments for their area of knowledge only. Answering from another person's perspective will take time and reflection at best, otherwise cognitive heuristics will cloud the assessment. The Performance Markers are written as objectively as possible, so that the results are reliable and quick to answer if answered honestly by the stakeholder. Stakeholders will need to conduct their own assessments, so that noise and bias is removed as far as possible.

Based on this analysis of the performance marker timings, I made some improvements to the wording of the associated performance markers, and these are described in the next section.

7.5.6 Changes to the wording of performance markers following the evaluation

The evaluation was conducted in two even parts. Both parts were conducted identically apart from the second part included minor changes to the wording of 3 performance markers. Following the evaluation of CAESAR8 in Part 1, I made changes to the wording of 3 of the 40 performance markers.

Based on my analysis of the timings that experts spent on questions for the performance markers (see Figure 7.11), I made changes to the wording of EF2 and HF3 to make them easier to understand:

EF2	Tested wording:	Stakeholder has considered their use of a third-party organization
	Revised wording:	Stakeholder is aware of their dependence on third-party organizations
HF3	Tested wording:	Stakeholder has reviewed results of user impact analysis for process and technology changes
	Revised wording:	Stakeholder has reviewed the results of user impact analysis for all changes

Although it was not related to timing analysis, and came from a response to the post-evaluation questionnaire, I also changed the wording of TI4 to specifically check for the execution of a documented test.

TI4	Tested wording:	Stakeholder is aware of a documented plan to test the changes to technology
	Revised wording:	Stakeholder confirms that testing is documented and executed satisfactorily

After part 2 of the evaluation, the analysis of the CAESAR8 assessment data was repeated to test how well the performance marker wording changes from part 1 had performed. The results of 213⁴ additional performance marker assessments are shown in Figure 7.12, which is a box-and-whisker plot showing how many seconds elapsed between questions. The box plot splits the data for each performance marker into quartiles, with the interquartile range forming the box. Again, the dividing line in the box is the median, and whiskers indicate the variability outside the upper and lower quartiles. The additional points shown are outlier values, for example, where an expert may have taken a break from the assessment.

(These graphs are generated directly from the web app's data storage, so the order that the performance markers appear in the box plots reflects the order that experts conducted their first assessments. Therefore, there will be some differences in the order of performance markers between the two separate box plots. For the purpose of this analysis, it was not required to readjust the orders.)

For ease of reference, red and green markers (up and down arrows) show a desired reduction in performance marker assessment median times between part 1 and part 2 of the evaluation for the reworded performance markers. The graph can also be compared directly with the same graph created for part 1 of the ex post evaluation process (see Figure 7.11). The average times for EF2, HF3 have now reduced (9 seconds and 13 seconds respectively). However, a potential issue with EF3 for some volunteers has reoccurred in part 2 (note the high upper quartiles in Figure 7.11 for EF3). This time, the average time taken has increased to 27 seconds. Analysis of the EF3 assessments does not show any particular reason for the increase, for example there were no long notes created for these assessments. A review of the wording identified that an improvement should be made to make the performance marker more easily understandable for all potential stakeholders.

⁴There were less assessments conducted in the second evaluation. This was partly due to one less volunteer finishing the evaluation in part 2 (see Table D.7) and a lower number of assessments per volunteer (a modal average of 2 for second part of the evaluation, as opposed to 3 for the first part of the evaluation).

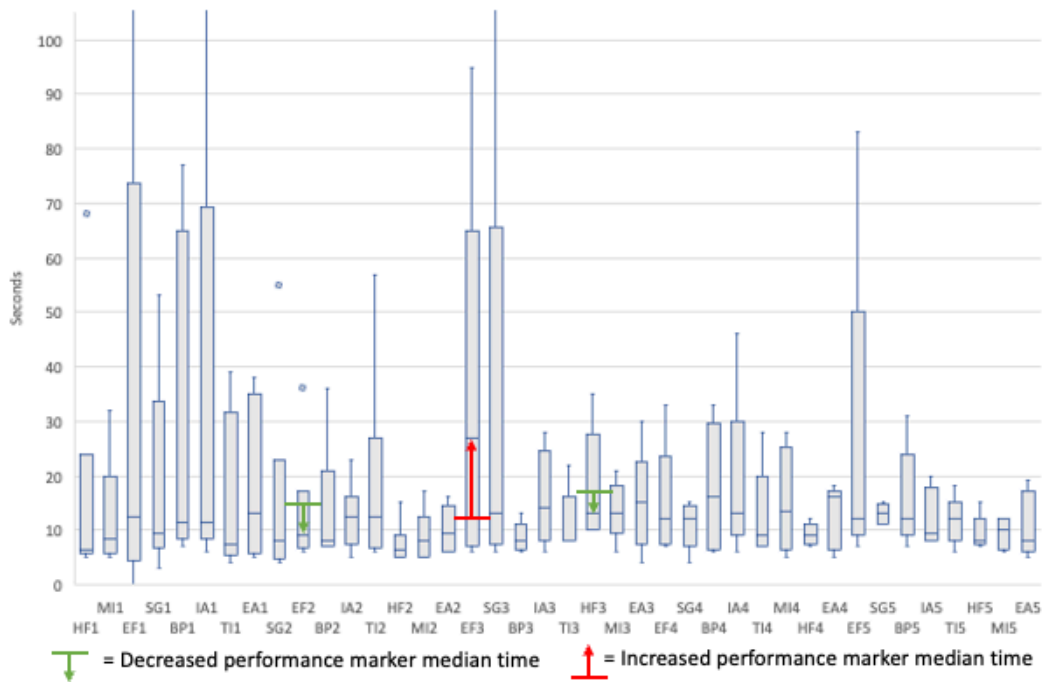


Figure 7.12: Box-and-whisker for user time-taken per performance marker in part 2 of the evaluation

EF3	Tested wording:	Resultant changes to stakeholder's security threats have been assessed
	Revised wording:	Stakeholder has checked for any consequential changes to security threats

I considered that the average time taken for all other assessments was reasonable. EA3 and BP4 had relatively high upper quartiles and median values, but analysis of the assessments has shown that the median was slightly elevated because *notes* were added by the expert during the performance marker assessment⁵. No further changes were made after altering the wording for these 4 performance markers. Therefore, overall, 10% of the full matrix of performance markers had their wording updated after part 2 of the evaluation; however the context of the performance marker, or its purpose, has not

⁵These notes actually explained how security impact assessments are often created retrospectively (EA3), and project managers are usually left to help stakeholders to identify business process changes, such as third party contracts, caused by the project (BP4). These comments show that the performance markers were understood and provide further evidence of the need for my contribution.

changed from that identified in the analysis.

All changes to performance markers have been made for version 2 of the question set contained in the CAESAR8 matrix, the latest copy of which can be found in Appendix E.

7.5.7 Further analysis and discussion of results

This section describes further analysis of the CAESAR8 evaluation results and discussion on some of the findings.

7.5.7.1 Collective decision-making

Whilst analyzing the evaluation results, I checked for diversity in the ratings that experts gave to the 15 common problem areas listed in the pre-evaluation questionnaire. I examined the correlations between the scores given by individual experts and also between the different expert types (Security, Business and Technical). A subset of the results is shown in Table 7.4.

Line #	Correlation	'r' Values
1	S1 and S2	0.23
2	S1 and S3	-0.13
3	S1 and S4	0.05
4	S2 and S3	0.15
5	S2 and S4	0.54
6a	S3 and S4	0.38
6b	S1 and S6	0.33
6c	S4 and S6	0.22
7a	S1 and (All-S1)	0.15
7b	S4 and (All-S4)	0.53
8	S1 and (B + T)	0.14
9	S and (B + T)	0.76
10	(S-S1) and (B + T)	0.69
11a	S4 and (B + T)	0.42
11b	S6 and (B + T)	0.38
12	S and ALL	0.96
13	(B + T) and ALL	0.91

Table 7.4: Correlation between experts' findings for the fifteen problem areas

I found that there was no correlation between the assessments of experienced professional security experts that volunteered to take part in the evaluation (depicted as 'S#' in Table 7.4). These differences relate to the experts' opinion on the problem areas for information security within business change projects.

It might be deduced from this that relying on a single security expert to identify all security issues and find the best solutions is most probably unrealistic. In fact, studies have shown that even the same individual can arrive at different judgments at different times [147]. For example, it has been shown that judicial rulings can be swayed by extraneous variables that should have no bearing on legal decisions [41]. It has been claimed that the decision may be based on "what the judge ate for breakfast" [100].

This finding has been evidenced in all types of professions. It has been found that the clinical decisions made in general practice are multifaceted, and not linear [118]. External factors of time, cost and media can all have an influence on a decision.

Using multiple security experts (e.g. Line 9) improves the result by filtering out potential anomalies, but the best results are achieved when the experts are from diverse backgrounds and bring their own specific knowledge and experience (e.g. Lines 12 and 13).

Section 6.3.2.2 provides more information on selecting stakeholders for CAESAR8 assessments.

7.5.7.2 Design style

I aimed to design an artifact that provides an element of style in its foundation and, therefore, encourage wide adoption within an organization. Hevner [72] quotes:

“Gelernter (1998) terms the essence of style in IS design machine beauty. He describes it as a marriage between simplicity and power that drives innovation in science and technology”.

In the words of one expert after completing their evaluation of CAESAR8:

“The assessments contain some powerful questions. The impact each set of assessment questions has on the result is really clear and very telling. I believe that it will make the process of initial evaluation of cyber security, and ongoing monitoring of cyber security related processes, understandable and easily accessible, even to small organizations with, potentially, a lesser basic understanding of cyber.” (T1)

The CAESAR8 model offers designers many opportunities to build a full information system that will encourage use by a wide range of stakeholders, while in the process delivering valuable benefits for security professionals and the wider organization. Please see Section 8.5 for a discussion on more development opportunities that should provide additional style.

7.6 Conclusion of Evaluation

The external evaluation of the CAESAR8 model was a summative evaluation that was carried out ex post of the CAESAR8 model design process. The evaluation was completed in two halves, and followed a three stage process: i) a pre-evaluation questionnaire; ii) a hands-on test of web app exemplar; and iii) a post-evaluation questionnaire. The evaluation was carried out by hand-picked experts who had more than ten years experience of working on information security projects in senior roles. The participants were selected for their diversity of knowledge (e.g., security professionals, business managers and technicians) and their veracious disposition on scientific matters that gave rigor to the evaluation.

In total, the evaluation process took five months to complete and required a high level of commitment from those that completed the process. Sixteen experts agreed to take part in the evaluation, of which fourteen started the process and eleven completed the process.

Responses to questionnaires confirmed that the problems for ISRM that I identified from the literature were correct and that the CAESAR8 model is helping to address them. As further evidence, the experts agreed that the subsequent design goals that I created for CAESAR8 had been achieved. The strongest design goals were: *The 40 questions [the performance markers] covered key issues to determine success*; and *It was valuable to include multiple stakeholders*. These design goals were central to my contribution and formed CAESAR8 design principles #2 and #3.

Although there was collective agreement that the fifteen problem areas were correct, I noted differences in how experts rated the severity of individual problems, especially between experienced information security experts. This fact provides additional evidence of the value of involving multiple, and ideally cognitively diverse, stakeholders in the ISRM process.

The questionnaires used a semi-open structure, meaning that each question included a free-text field, and many positive comments were volunteered about the CAESAR8 model's value as a practical solution for SME organi-

zations. However, no additional problem areas were added to the fifteen that I identified from the literature.

The web app developed for the evaluation gave experts first-hand experience of how the model functions. It was designed to be used with desktop browsers and one expert, who did not complete the evaluation, referred to the fact that it was not optimized for mobile phones. On reflection, it would have been beneficial to design the web app to fully support both desktop and mobile formats, so that participants could use their preferred devices. My instructional video ensured that all participants received the same level of training on the web app. After analyzing the web app data, I changed the wording of three performance markers to improve operational efficiency.

Chapter 8

Conclusion

Following Design Science Methodology, I have designed a novel model called CAESAR8 that helps to manage information security risks under the constraints experienced within agile business change projects. This model takes an holistic approach to assessing the information security impact across multiple departments and business functions, and examines the main indicators for a successful information security strategy by focusing on key performance markers. By reviewing the progress across eight domains and five levels of the model, CAESAR8 can help organizations avoid many of the common pitfalls for information security. This is achieved without the need for prior assurance activities that may otherwise hinder agile development.

Multiple stakeholders complete individual CAESAR8 assessments in their own time and space. These assessments are then aggregated and the combined results are calculated using a set of custom rules. The results are then presented in an intelligible, visual dashboard that can be shared at all levels of the organization.

My evaluation of the artifact was conducted *ex ante* and *ex post*. The *ex ante* evaluation was conducted using case studies during the design of the artifact.

The Gangs Matrix case study used in the *ex ante* evaluation was a real-life scenario in the form of a fully documented data breach, see Section 6.4.2. This work showed that the model was able to identify all of the known in-

formation security breaches for the given scenario. The case study has also demonstrated the power of aggregating the assessments from different stakeholders to provide a combined perspective, see Section 5.5.2.

An ex post evaluation was then conducted at the end of the study using a group of industry experts who had diverse knowledge, perspectives and heuristics. To support the evaluation, the model was presented in a web app, which also demonstrated how the model can be realized within a business environment. After using the model, the experts confirmed that CAESAR8 will improve how projects can identify and support the treatment of information security risks and address real-world problems in projects.

CAESAR8 can be used to provide a rapid and holistic assessment of information security requirements in a project at any stage of its development. The benefits of using the model begin from the start of a project. CAESAR8 can be used standalone or to support the work of project managers, security professionals and architects. By conducting incremental reviews, key issues can be uncovered at an early stage of project iterations. If used continuously, CAESAR8 encourages the development of a working vision for an information security architecture within an agile team. The model can also support the maintenance of existing enterprise information security architecture, by incorporating checks for important just-in-time documentation.

One of the strongest benefits highlighted in the evaluation of CAESAR8 by experts is the involvement of multiple, independent stakeholders in the overall assessment. This is a novel approach for information security that combines existing research in behavioral science with an innovative design for managing information security in agile business change projects. This is a key concept for improving information security risk assessments.

CAESAR8 can also be used to assess Operational Technology (OT) projects as well as information security projects, and it can provide an integrated perspective of safety and security. This is a benefit of the CAESAR8 model's ability to assess multiple business perspectives in a concurrent process, showing how safety and security can be considered in unison, so that the effects of security can be evaluated and treated in the wider context of safety.

8.1 A review of the five CAESAR8 design principles

My research has confirmed the theoretical benefits of enterprise architecture (EA) approaches for information security risk management (IRSM) but uncovered problems for all organizations trying to achieve this in practice. I have therefore developed a new model, which I have called CAESAR8, to assist small-to-medium sized enterprises (SME) in achieving agile EA approaches to IRSM.

This section describes how the CAESAR8 design principles have been met by the final artifact's design.

8.1.1 Principle 1: Base artifact on a practical, holistic design

I have identified fifteen problem areas and nine underlying issues from my research into the performance of information security risk management. I designed the CAESAR8 model to help overcome these problems in business change projects in an agile and holistic way. These problems have been confirmed by a diverse group of experienced professionals during the evaluation of the CAESAR8 model; and these experts have agreed that the CAESAR8 design objectives have been met.

8.1.2 Principle 2: Gather multiple stakeholder perspectives

Human behavioral-science has demonstrated that teams can arrive at more accurate judgments if the team has diversity in knowledge and experience in relation to a given task. CAESAR8 incorporates this research into its design. For any given risk assessment, it obtains multiple but independent assessments of the CAESAR8 matrix from all those stakeholders who are affected by a proposed business change. Using this design principle, the model captures the tacit knowledge of those individuals who have the best under-

standing of the local impact of the change.

These individual assessments are then combined into a single result. Rules for the consolidation process have been provided that ensure the views of all stakeholders are preserved for further discussion.

This process also ensures that stakeholders are actively and continually involved in the enterprise architecture, and it avoids the dangers of *groupthink*, where a consensus is often reached based on the views of a central individual who often lacks crucial knowledge.

Another positive consequence of distributed assessments is that CAESAR8 also allows stakeholders to participate in the process regardless of different time zones and geography. There is no need for all stakeholders to be present in the same place and at the same time when they take part in a joint CAESAR8 assessment (in fact, they should not be).

8.1.3 Principle 3: Unify around a tractable checklist

By conducting root cause analysis of IS failures, eight domains have been identified that categorize how enterprises should assess the progress of their business change projects in relation to ISRM, and five levels that determine the sequence in which the elements of each domain should be considered. Together, these two dimensions form the CAESAR8 matrix. The CAESAR8 matrix also provides the framework for an Agile Enterprise Information Security Architecture (A-EISA).

Each of the 40 cells in the CAESAR8 matrix contains a performance marker (question) that all stakeholders in a project can assess to determine the impact of business change in relation to ISRM. These performance markers have been determined from pairwise analysis of the root causes of IS failures. By conducting continual reviews of progress on these factors, the maturity of information security strategies can be constantly reassessed to provide a real-time metric.

8.1.4 Principle 4: Value process over EA artifacts

Organizations can use the CAESAR8 model to improve EA implementations or can use the model standalone to ensure that projects are managing enterprise risks during business change projects. CAESAR8 is particularly suited to environments where human resources may already be stretched to the limits, as CAESAR8 assessments are performed expeditiously and with no requirement to create EA artifacts.

8.1.5 Principle 5: Provide a collective visualization

I have created CAESAR8 as a cyclical design to reinforce its purpose as a continuous assessment and I describe how this is crucial for use in agile projects. I have included the most appropriate form of metrics to engage a diverse group of stakeholders and elicit positive intervention by senior business executives to treat security risks adequately as projects evolve. The output of the model is presented as a radial diagram, which has been identified as providing the most suitable format for communicating the results of CAESAR8 assessments, as it helps to ensure that key information is instantly understood.

The thesis describes how to use CAESAR8 in a business environment and how to present the results. Further development opportunities are described that will make the presentation more interactive.

8.2 CAESAR8 in the context of EA theories

Despite the concepts of EA having existed for many years, successful EA implementations do not resemble the recommendations of current frameworks [98]. Kotsuev et al. explain that in practice, EAs do not follow the step-wise linear processes that popular frameworks and methodologies propose (e.g., TOGAF [64] and Zachman [184]) but have been implemented by a complex constellation of activities. Their practicality has therefore been assumed, rather than proven to work.

Kotusev et al. [98] describe 10 theories (see Table 2.15) that explain how EA artifacts work in practice. Practical problems associated with these theories suggest a systemic issue with the current EA concept that is preventing its wider adoption within business and meaning that the full benefits of EA are not widely exploited by many organizations, and this state could potentially exist for some time to come.

It is important that the information security strategy complements any existing EA, but it should drive forward its own requirements for the EISA. It should not simply play a ‘bit-part’ of existing EA, as this will not meet the dynamic needs of an effective information security strategy.

The 10 theories proposed by Kotusev et al. [98], see Table 2.15, highlight the need for the practical business solution that my research has designed. CAESAR8 is designed to encourage an holistic process is followed, rather than focusing on specific EA artifacts, however, the benefits of CAESAR8 is often achieved in a way that is synonymous with the practical guidance which they provided. I make the following observations about seven of the theories that they have developed and how CAESAR8 helps to accomplish these:

- **Actor-network theory:** *Describes the usage of EA artifacts for communication between different organizational levels.*

There is a potential concern that relying on the need for more proactive approaches to build the architecture top-down could be seen as a hindrance for the adoption of agile values, e.g. , “Responding to change over following a plan”. My model supports the reactive needs of modern organizations as decisions do not need to “trickle down” to shape perspectives lower down the hierarchy. This also helps to protect the accuracy of risk assessments and encourages innovation.

- **Uncertainty Principle, a component of the Usability Theories:** *Describes the fact that global, long-term planning is supported by very abstract EA artifacts.*

My model does not require organizations to construct the big picture, and there is no expectation that artifacts will need to be made “con-

crete”. My model places more emphasis on the EA process, rather than the EA artifact (i.e., the journey, rather than the destination), but encourages teams to create and review artifacts dynamically as the need arises, such as to support the *Boundary objects theory* described in Table 2.15. In this way, my model builds-out the architecture. This is more supportive of agile and lean methodologies and is more attuned to embracing the increasing complexities of IT – e.g., cloud and IoT.

- **Communities of practice theory:** *Describes the place and usage of EA artifacts in the organizational social landscape.*

By incorporating stakeholder assessments directly, my model provides virtual communities of practice, where “ivory towers” cannot exist, as progress is measured collectively for the whole community based on a *worst-case* scenario. Allowing stakeholders to perform an assessment independently means that my model also helps to remove cognitive biases, such as the tendency to conform to a consensus in face-to-face meetings.

- **Knowledge Management:** *Describes different usage of EA artifacts capturing IT landscapes and business visions.*

My model captures the tacit knowledge of stakeholders by incorporating their perspectives in real-time assessments of current changes to the architecture.

- **Media richness theory:** *Describes different communication patterns for EA artifacts reflecting opinions and facts.*

My model pools the opinions of all stakeholders and presents this analysis in real-time, and can be instantly shared at all levels of the enterprise hierarchy. This supports *Decision-making theories* described below.

- **Decision-making theories:** *Describe the participation of stakeholders in the creation of future-focused EA artifacts.*

Stakeholders themselves become virtual architects in the CAESAR8 process and are therefore incentivised to take ownership of artifacts and collaborate, even when they may be used to working autonomously. In

this way, the model balances the conventional top-down hierarchy with a bottom-up approach, to ensure that enterprise architecture is not something that is done to individuals down-stream – the hazards of which are clearly presented in the research of Kotsuev et al.

- **Management fashion theory:** *Describes dramatic differences between recommended and actual usage of EA artifacts.*

My model is based on novel research into the root causes of common failures and successes. It has not been aligned to any existing EA framework or security standard because such frameworks maybe unproven - a point well made by Kotsuev et al.

CAESAR8 reinforces the concept of “*process over artifact*” when providing holistic information security risk assessments by virtue of its forth design principle (Principle 4: Value process over EA artifacts). This approach supports the *building out* of an EA, rather than prescribing it on the business. As a tool for providing continuous improvement of ISRM, CAESAR8 supports the mantra that it is “*the journey that is most important, rather than the destination*”. In other words, maintain an accurate understanding of risks as the business goes through change, rather than focusing on completing a risk register or documenting an EA.

8.3 CAESAR8 and NIST organizational risk management

The National Institute of Standards and Technology (NIST) has published Special Publication 800-39, titled: Managing Information Security Risk - Organization, Mission, and Information System View. This is their flagship document in the series of information security standards and guidelines to provide guidance for an integrated, organization-wide program for managing information security risk to organizational operations.

The NIST standard for managing information security risk [80] describes a three-tier approach for organizational security risk management. The tiers are described as the: (i) organization level; (ii) mission/business process level; and (iii) information system level. CAESAR8 supports this multi-tiered approach by ensuring that the risk management process is carried out within and across the three tiers by involving all stakeholders that have a direct involvement in the specific business objectives. The results of their assessments can be summarized at the appropriate tier.

In particular, CAESAR8 provides the NIST *feedback loop for continuous improvement*. This important feedback will help reduce the uncertainty that organizations often experience as to how risk management is actually performing [162]. See Figure 8.1. Information is provided to Tier 1 from the lower tiers so that risk-based decisions can be made and then delivered back to the lower tiers for action.

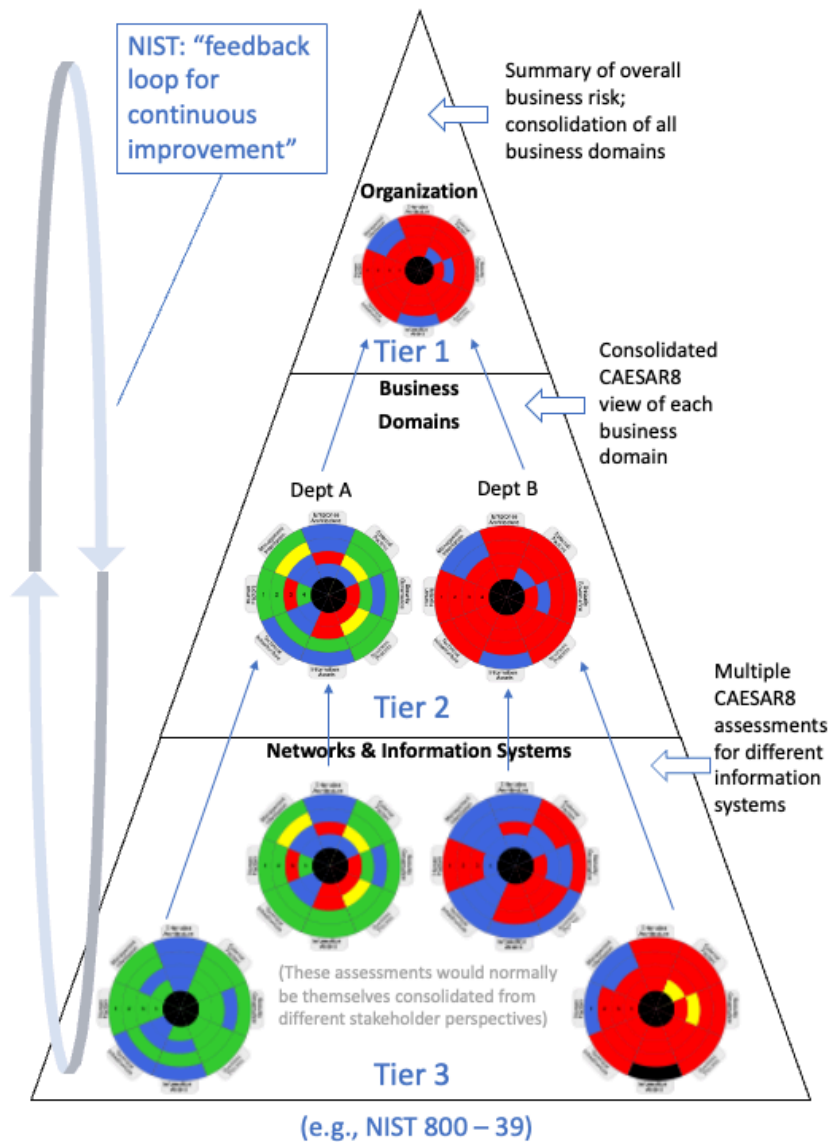


Figure 8.1: Multitiered organizational-wide risk management using CAESAR8 for a NIST Publication 800-39

This is precisely how CAESAR8 has been designed to operate. The CAESAR8 model will handle the intra-tier assessments (which maintains integrity as described in the thesis) and consolidate the lower tier assessments to provide the management information, in the form of a combined assessment for the respective middle tier’s information systems. The combined results are then presented to the higher tiers. Figure 8.1 shows how the process

works. This provides an important *closed loop* system for risk management. The NIST document describes how: “*making information security-related requirements and activities an integral part of the system development life cycle ensures that senior leaders/executives consider the risks to organizational operations and assets, individuals, and other organizations.*” [80], but NIST also describe how it is a fundamental requirement that the senior management support the concept of organizational-wide risk management and allow it to operate as an integral part of operations in cyberspace. Section 6.3.3 provided a description of how this also forms a key requirement of the CAESAR8 implementation principles.

In their document, NIST also highlight the importance that EA performs in managing information security risks. They make the following point: “*The use of enterprise architecture can greatly enhance an organization’s risk posture by providing greater transparency and clarity in design and development activities.*” [80]. Whilst their comment specifically relates to the implementation of commercial EA frameworks, CAESAR8 will assist in achieving these principles reliably, regardless of what EA may, or may not, be in place for an organization. Whilst many organizations are unable to facilitate the necessary EA maintenance during projects (e.g. the creation and updating of EA artifacts), CAESAR8’s agile design will help organizations to achieve this, if it is required.

The inter-tier communications for higher management decisions will require a separate reporting method to ensure reliability of risk decisions between the tiers. This can be achieved in a lean format, in a similar manner to that pioneered by Toyota [107]. An example is shown in Figure 8.2.

Note that the higher tiers (Tier 1 and Tier 2), are calculated by consolidating two or more assessments at Tier 3, the lower tier, so that the results fed back to the higher tiers are a truly accurate representation of risk.

Further, it must be recognized that CAESAR8 is a continuous assessment, so all of the results need to be calculated in real-time. Any saving and re-use of results could lead to inaccurate data being used for the reports. Therefore, the reports need to be generated dynamically.

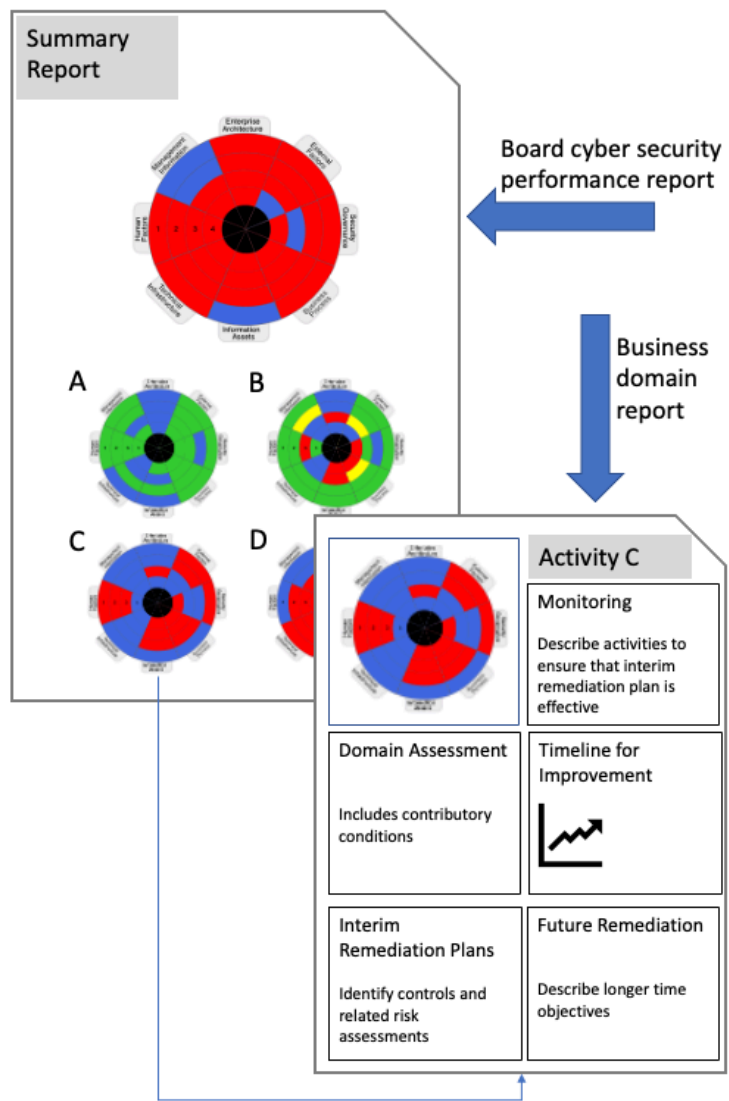


Figure 8.2: Example metrics reporting based on Lean concepts

8.4 Limitations of CAESAR8

My final artifact is a model that can be used for conducting holistic reviews of information security risks in real-time. However, it will require that an application is developed to provide these benefits to an organization.

CAESAR8 is not a strategic planning tool for achieving a target enterprise architecture. EA frameworks and EA artifacts that are documented to the

relevant level of detail may still be required for this purpose.

The CAESAR8 model provides a generic assessment in relation to the overall status of information security risks, but it does not attempt to define what the individual risks are in detail. It still requires the skills of individual stakeholders and SMEs, using their own standards and tools, to determine how to respond to specific performance markers. This is potentially a different process for different stakeholders.

CAESAR8 provides the consolidated output, but the results will probably need to be included in a report. This still needs to be designed and should probably provide senior executives of the company with trend information, so that the direction of travel is clear. An example report is included in this thesis and is based on lean concepts (see Section 8.3).

I also highlight an unavoidable limitation of the evaluation process. A basic instantiation of the model was developed to facilitate the evaluation. However, the evaluation process was still very time-intensive for volunteers as they were required to complete two questionnaires and conduct tests of the web app instantiation of the artifact. This provided rigor to the evaluation but was a very time consuming process, both for participants and to manage the process. Therefore, volunteers were carefully selected for their experience and diversity to ensure a rigorous evaluation of the artifact. Whilst a sufficient number of volunteers needed to be sought, the overall volume of volunteers was not the primary objective in this regard.

It is beyond the scope of this research to create a full, commercial product. This would have been a necessary step to provide a full *in situ* business evaluation of the model (Section 8.5 describes some further development opportunities). The web app created for the evaluation was only a basic instantiation that allows experts to test the model's core design characteristics, and determine if they believed that the design goals had been met. Using the web app, volunteers have tested the model based on scenarios that are familiar to them.

The time required for stakeholders to learn a more complex instantiation of the model would have increased training time, resulting in an overall in-

crease in time to complete the evaluation. A more complex instantiation might have also detracted from the main purpose of the evaluation, which was to evaluate the model and its core design principles, rather than the particular instantiation.

8.5 Further Development Opportunities

For a practical business solution, further development of the model will be required, but this is possible by making a process of incremental improvements over the basic core design of the exemplar. An application of CAESAR8 would clearly need to incorporate a full authentication and access control environment for users and administrators of the artifact, and this could include the global configuration of organizational risk assessments and/or current change programs/projects. It could also include the ability for administrators to send invitations and reminders to stakeholders, and obtain a global picture on the current status of ongoing discussions.

One of the key enhancements that could be added to a CAESAR8 application is an animation of stakeholder activity, to provide key management information, but also to encourage a commitment of continual reviews by all stakeholders. This animation was discussed in the **Design Style** Section 7.5.7.2, and concerns overlaying *orbiting electrons* onto the graphical results to show where stakeholders are currently reviewing performance markers (the electrons orbit the current track). The speed of rotation could be based on an algorithm that calculates the stakeholders activity, such as the time spent in the model, the last time a change was made, and the volume of changes. For an administrator examining the results of a consolidation of multiple stakeholder assessments, there would be multiple electrons with a corresponding label showing which particular stakeholder the electron represents. For individual users/stakeholders, if the assessment is being included in a consolidation with other assessments, the other stakeholders current activity for those other assessments could also be displayed in a ‘greyed’ out style, to provide evidence and encouragement to the current stakeholder.

EA artifacts (e.g. tables and diagrams describing the enterprise) could be stored or linked within the assessments and shared as part of the assessment process. These could be updated when approved and stored back to a repository with version control incorporated. Stakeholders could have the ability to share these artifacts and conduct online discussions/consultations regarding the necessary changes.

The current results could automatically populate a management report, and even show the direction of travel, i.e., the trend. Section 8.3 includes details of an example report that is based on tested lean concepts.

An import/export facility could be added to allow assessments to be completed offline - e.g., to support a field assessment on a tablet, and then imported back to the CAESAR8 system.

To support color-blind readers or black and white printed reports, the letters of R, A, G and B could also be shown in the result sectors, with blank being unanswered and N/A shown as completely blacked out in the usual way. Alternatively, the colors for the model could be selected from color blind friendly palettes.

A CAESAR8 application could provide warnings for any unexpected results. This could simply be if everyone is *trusting* someone else, for example. However, this could be implemented for specific scenarios. For example, if 'Trust' has been selected by a stakeholder for MI5, which is that stakeholder's own security culture posture, raise an alert and/or show an exclamation mark (!) in the corresponding results sector. In this example, the stakeholder is asking someone else to provide evidence back to them about their own security culture. This could be true but should be clarified.

It would also be helpful to include a facility for a stakeholder to propose other stakeholders that should conduct a separate assessment from their own perspective for the business change proposal. Stakeholders would originally be selected from the center, such as by a CISO or Product Manager, but a stakeholder may have greater knowledge about who they need to rely on and where their particular jurisdiction ends. In other words, they maybe *trusting* another stakeholder, who has not yet been identified, to ensure that their own business function is successful.

This concept could also be extended to allow stakeholders to specify who they are actually trusting. If that other stakeholder provides a *Yes* value for a CAESAR8 Performance Marker it would then change the trusting stakeholder's result to a *Yes* for the purposes of the consolidation. To protect CAESAR8 integrity, the trusting stakeholder would need to select this dependency. It should not be selected on their behalf.

The CAESAR8 results could have interactive features and one of these could be the selection of a sector¹, or multiple sectors, to see details of the assessment or change values. However, changing a value needs to be done with caution, since the results for prior levels are significant for CAESAR8 assessments. Individual performance markers are arranged to respect the process and not the final result. Returning the user to the full assessment would be a better design option for CAESAR8. However, if the results included some of the additional warnings described in this section, it would be an effective way of navigating the results.

Note that some of the volunteer experts that took part in the evaluation phase of my research suggested adding configurable questions. I recommend that this is added as another layer, so that the performance markers are always present but can be extended (e.g. HF1a and HF1b, etc.).

8.6 Future Research Opportunities

An important but separate exercise required for CAESAR8 is the selection of stakeholders. Further research could be undertaken to determine how this section process could be made easier, or even standardized.

The performance markers were created based on research into the generic study information security incidents but further research could determine whether they could be optimized or adapted to specific scenarios. For example, further scientific research could be conducted into specific business domains to see if the performance markers could be optimized for certain applications, or even specific systems. A potential area for further research

¹These have been described as selection tools for a radial diagram design [182]

is to ensure that this checklist is optimized. For example, one expert in the evaluation process recommended adding editable milestones that would make the model contextual to an organization. This could be valuable, although it is worth recalling a phrase that is especially true for the operation of CAESAR8: “it’s the journey that is important, not the destination”. However, such milestones could be displayed on the model as a new feature that overlays the current process.

This research could also include further studies of CAESAR8’s use in Operational Technology (OT). This can be used to address the growing concern that security risks can have in the physical world [169] and is a promising area of further research.

Further research could include a study of how to best present the results of CAESAR8 so that the trend in results can be identified.

Further research could also be conducted into the benefits of using CAESAR8 as an assessment tool for the wider enterprise, and not just business change projects. CAESAR8 could have the ability to pre-select the categorization of assessments to discover the risk profile for different systems and/or departments, or the global (i.e., organizational) effect of change. Assessments can be combined in multiple ways to discover the where the risks of changes have the greatest impact, however, these combinations must always be recalculated from the original stakeholder assessments, i.e., it is not acceptable to discover the overall risk for a department by management conducting a separate risk assessment.

Likewise, summary assessments should not be saved and used as part of a different assessment, otherwise the real risk will not be recalculated. In this way, *what-if* analysis is supported, but the calculations remain dynamic.

The scope of the categorization should always be defined (just like any unit of measurement), so that the results are unambiguous. Observe the NIST discussion in Section 8.3: Tier 1 and Tier 2 represent where categorization can take place, but the scope of the consolidation/categorization must be clear - e.g., is this an assessment for a single system change or the overall status for a department, or the organizational change program? This must be clearly defined and stated. Users of a CAESAR8 system may then be

given the ability to configure how the assessments are presented, e.g., by level or domain.

A stakeholder activity indicator, such as the orbiting electrons discussed in the previous section, is intended to encourage greater involvement from all stakeholders. There could also be other features added to encourage stakeholder involvement, such as a daily prompt to review a specific aspect of the assessment. At the end of a week, a full assessment has then been completed.

Bibliography

- [1] Vipindev Adat and B. B. Gupta. Security in Internet of Things: issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, 67(3):423–441, March 2018.
- [2] Atif Ahmad, A. B. Ruighaver, and W. T. Teo. An information-centric approach to data security in organizations. In *TENCON 2005 2005 IEEE Region 10*. IEEE, 2005.
- [3] Areej AlHogail and Jawad Berri. Enhancing it security in organizations through knowledge management. In *Information Technology and e-Services (ICITeS), 2012 International Conference on*, pages 1–6. IEEE, 2012.
- [4] Abdullah Almubark, Nobutoshi Hatanaka, Osamu Uchida, and Yukiyo Ikeda. Identifying the organizational factors of information security incidents. In *2015 Second International Conference on Computing Technology and Information Management (ICCTIM)*, pages 7–12. IEEE, 2015.
- [5] C Andrews, C Monk, and R Johnston. Integrated architecture framework and security risk management for complex systems. 2014. IET.
- [6] Louis Anthony (Tony) Cox Jr. What’s wrong with risk matrices? *Risk Analysis: An International Journal*, 28(2):497–512, 2008. Wiley Online Library.

- [7] A. G. Asuero, A. Sayago, and A. G. González. The Correlation Coefficient: An Overview. *Critical Reviews in Analytical Chemistry*, 36(1):41–59, January 2006.
- [8] Pavel Atanasov. Small steps to accuracy_ Incremental belief updaters are better forecasters. *Organizational Behavior and Human Decision Processes*, page 17, 2020.
- [9] Serap Atay and Marcelo Masera. Challenges for the security analysis of Next Generation Networks. *Information security technical report*, 16(1):3–11, 2011.
- [10] Michael Atighetchi, Paul Rubel, Partha Pal, Jennifer Chong, and Lyle Sudin. Networking aspects in the DPASA survivability architecture: An experience report. In *Network Computing and Applications, Fourth IEEE International Symposium on*, pages 219–222. IEEE, 2005.
- [11] Colin Atkinson, Christian Cuske, and Tilo Dickopp. Concepts for an Ontology-centric Technology Risk Management Architecture in the Banking Industry. In *Enterprise Distributed Object Computing Conference Workshops, 2006. EDOCW'06. 10th IEEE International*, pages 21–21. IEEE, 2006.
- [12] David H Autor, Frank Levy, and Richard J Murnane. The skill content of recent technological change: An empirical exploration. *The Quarterly journal of economics*, 118(4):1279–1333, 2003.
- [13] C Warren Axelrod and CISSP CISM. Accounting for value and uncertainty in security metrics. *Information Systems Control Journal*, 6:1–6, 2008.
- [14] Abdul Ghani Azmi, Ida Madieha, Sonny Zuhuda, and Sigit Puspito Wigati Jarot. Data breach on the critical information infrastructures: Lessons from the Wikileaks. In *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on*, pages 306–311. IEEE, 2012.

- [15] Faezeh Bahmani, Marzieh Shariati, and Fereidoon Shams. A survey of interoperability in Enterprise Information Security Architecture frameworks. In *Information Science and Engineering (ICISE), 2010 2nd International Conference on*, pages 1794–1797. IEEE, 2010.
- [16] Ryan SJD Baker. Gaming the system: A retrospective look. *Philippine Computing Journal*, 6(2):9–13, 2011.
- [17] Kent Beck, Mike Beedle, Arie Van Bennekum, Alistair Cockburn, Ward Cunningham, Martin Fowler, James Grenning, Jim Highsmith, Andrew Hunt, Ron Jeffries, et al. Manifesto for agile software development. 2001.
- [18] Soukayna Belkadi, Ilias Cherti, and Mohamed Bahaj. Lean in information technology: Produce the human before the software. In *International Conference on Advanced Intelligent Systems for Sustainable Development*, pages 203–213. Springer, 2018.
- [19] Konstantin Beznosov and Philippe Kruchten. Towards agile security assurance. In *Proceedings of the 2004 workshop on New security paradigms*, pages 47–54. ACM, 2004.
- [20] Sanjay Bhasin. An appropriate change strategy for lean success. *Management Decision*, 2012.
- [21] Ken Birman. The untrustworthy web services revolution. *Computer*, 39(2):98–100, 2006.
- [22] Stefan Bischoff, Stephan Aier, and Robert Winter. Use it or lose it? the role of pressure for use and utility of enterprise architecture artifacts. In *2014 IEEE 16th Conference on Business Informatics*, volume 2, pages 133–140. IEEE, 2014.
- [23] R Scott Bittler and G Kreizmann. Gartner enterprise architecture process. *Evolution*, 21, 2005.

- [24] Boeing. 737 MAX updates. <https://www.boeing.com/commercial/737max/737-max-update.page>, 2019.
- [25] Rok Bojanc and Borka Jerman-Blažič. An economic modelling approach to information security risk management. *International Journal of Information Management*, 28(5):413–422, October 2008.
- [26] Louis J. Bottino. Security Measures in a Secure Computer Communications Architecture. In *25th Digital Avionics Systems Conference, 2006 IEEE/AIAA*, pages 1–18. IEEE, 2006.
- [27] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.
- [28] Jakub Breier and Ladislav Hudec. Risk analysis supported by information security metrics. In *Proceedings of the 12th International Conference on Computer Systems and Technologies*, pages 393–398, 2011.
- [29] Glenn M. Brunette Jr and Christoph L. Schuba. Toward systemically secure IT architectures. In *Enabling Technologies: Infrastructure for Collaborative Enterprise, 2005. 14th IEEE International Workshops on*, pages 8–15. IEEE, 2005.
- [30] Jason S. Burkett. Business Security Architecture: Weaving Information Security into Your Organization’s Enterprise Architecture through SABSA®. *Information Security Journal: A Global Perspective*, 21(1):47–54, January 2012.
- [31] Ada Hui-Chuan Chen, Huei-Chung Chu, and Sou-Chein Wu. Against the breaches: Data loss prevention for online travelling services. In *Information Security and Intelligence Control (ISIC), 2012 International Conference on*, pages 282–285. IEEE, 2012.
- [32] Howard Chivers, Richard F. Paige, and Xiaocheng Ge. Agile Security Using an Incremental Security Architecture. In Hubert Baumeister, Michele Marchesi, and Mike Holcombe, editors, *Extreme Programming*

- and Agile Processes in Software Engineering*, Lecture Notes in Computer Science, pages 57–65. Springer Berlin Heidelberg, 2005.
- [33] Kim-Kwang Raymond Choo. The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8):719–731, November 2011.
- [34] J. Collmann and T. Cooper. Breaching the Security of the Kaiser Permanente Internet Patient Portal: the Organizational Foundations of Information Security. *Journal of the American Medical Informatics Association*, 14(2):239–243, March 2007.
- [35] Andrew M Colman. *A dictionary of psychology*. Oxford quick reference, 2015.
- [36] Information Commissioner. Metropolitan police service enforcement notice - ico. <https://ico.org.uk/media/action-weve-taken/enforcement-notice/2260336/metropolitan-police-service-20181113.pdf>, 2018.
- [37] Deborah L Cooper. Data security: data breaches. In *Proceedings of the 2015 Information Security Curriculum Development Conference*, pages 1–3, 2015.
- [38] Laura Corriss. Information security governance: Integrating security into the organizational culture. In *Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies*, pages 35–41, 2010.
- [39] Bruno Silveira Cruz and Murillo de Oliveira Dias. Crashed boeing 737-max: fatalities or malpractice. *GSJ*, 8(1):2615–2624, 2020.
- [40] Adéle Da Veiga and Jan HP Eloff. A framework and assessment instrument for information security culture. *Computers & Security*, 29(2):196–207, 2010.
- [41] Shai Danziger, Jonathan Levav, and Liora Avnaim-Pesso. Extraneous factors in judicial decisions. *Proceedings of the National Academy of Sciences*, 108(17):6889–6892, 2011.

- [42] Robyn M Dawes. The robust beauty of improper linear models in decision making. *American psychologist*, 34(7):571, 1979.
- [43] Jeroen De Mast and Joran Lokkerbol. An analysis of the six sigma dmaic method from the perspective of problem solving. *International Journal of Production Economics*, 139(2):604–614, 2012.
- [44] Robson de Oliveira Albuquerque, Luis Villalba, Ana Orozco, Fábio Buiati, and Tai-Hoon Kim. A Layered Trust Information Security Architecture. *Sensors*, 14(12):22754–22772, December 2014.
- [45] Ahmed Deif. Assessing lean systems using variability mapping. *Procedia Cirp*, 3:2–7, 2012.
- [46] Thomas Diefenbach, Carsten Lucke, and Ulrike Lechner. Towards an Integration of Information Security Management, Risk Management and Enterprise Architecture Management – A Literature Review. In *2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, pages 326–333, December 2019. ISSN: 2330-2186.
- [47] Stephan Diehl, Fabian Beck, and Michael Burch. Uncovering strengths and weaknesses of radial visualizations—an empirical approach. *IEEE Transactions on Visualization and Computer Graphics*, 16(6):935–942, 2010.
- [48] Rainer Diesch, Matthias Pfaff, and Helmut Krcmar. A comprehensive model of information security factors for decision-makers. *Computers & Security*, 92:101747, 2020.
- [49] V. Dorca, R. Munteanu, S. Popescu, A. Chioreanu, and C. Peleskei. Agile approach with Kanban in information security risk management. In *2016 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR)*, pages 1–6, May 2016.

- [50] Geoffrey M Draper, Yarden Livnat, and Richard F Riesenfeld. A survey of radial methods for information visualization. *IEEE transactions on visualization and computer graphics*, 15(5):759–776, 2009.
- [51] Bob Duncan and Mark Whittington. Information security in the cloud: should we be using a different approach? In *2015 IEEE 7th International Conference on Cloud Computing Technology and Science (Cloud-Com)*, pages 523–528. IEEE, 2015.
- [52] Suhazimah Dzazali, Ainin Sulaiman, and Ali Hussein Zolait. Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. *Government Information Quarterly*, 26(4):584–593, October 2009.
- [53] Csilla Farkas and Michael N. Huhns. Securing enterprise applications: Service-oriented security (SOS). In *E-Commerce Technology and the Fifth IEEE Conference on Enterprise Computing, E-Commerce and E-Services, 2008 10th IEEE Conference on*, pages 428–431. IEEE, 2008.
- [54] Bassam S. Farroha and Deborah L. Farroha. 7.6. 3 Architecting a Secure Enterprise Data Sharing Environment to the Edge. In *INCOSE International Symposium*, volume 21, pages 984–989. Wiley Online Library, 2011.
- [55] Stefan Fenz, Andreas Ekelhart, and Edgar Weippl. Fortification of IT Security by Automatic Security Advisory Processing. In *22nd International Conference on Advanced Information Networking and Applications (aina 2008)*, pages 575–582. IEEE, 2008.
- [56] Daniel J Fernandez and John D Fernandez. Agile project management—agilism versus traditional approaches. *Journal of Computer Information Systems*, 49(2):10–17, 2008.
- [57] Fabian Gampfer, Andreas Jürgens, Markus Müller, and Rüdiger Buchkremer. Past, current and future trends in enterprise architec-

- ture—A view beyond the horizon. *Computers in Industry*, 100:70–84, September 2018.
- [58] Atul Gawande. The checklist manifesto: How to get things right. *Journal of Nursing Regulation*, 1(4):64, 2011.
- [59] Michael L George, John Maxey, David T Rowlands, and Malcolm Upton. *Lean six sigma pocket toolbox*. McGraw-Hill Professional Publishing, 2004.
- [60] Hamza Ghani, Jesus Luna, and Neeraj Suri. Quantitative assessment of software vulnerabilities based on economic-driven security metrics. In *2013 International Conference on Risks and Security of Internet and Systems (CRiSIS)*, pages 1–8. IEEE, 2013.
- [61] Jamshid Gharajedaghi. *Systems thinking: Managing chaos and complexity: A platform for designing business architecture*. Elsevier, 2011.
- [62] Joseph Goldberg and Jonathan Helfman. Eye tracking for visualization evaluation: Reading values on linear versus radial graphs. *Information visualization*, 10(3):182–195, 2011.
- [63] Wilson Goudalo and Dominique Seret. The Process of Engineering of Security of Information Systems (ESIS): The Formalism of Business Processes. pages 105–113. IEEE, 2009.
- [64] The Open Group. *TOGAF Version 9.1*. van Haren Publishing, Zaltbommel, 10th new edition edition edition, November 2011.
- [65] Saikat Guha and Srikanth Kandula. Act for affordable data care. In *Proceedings of the 11th ACM Workshop on Hot Topics in Networks*, pages 103–108. ACM, 2012.
- [66] B. B. Gupta, Shashank Gupta, and Pooja Chaudhary. Enhancing the Browser-Side Context-Aware Sanitization of Suspicious HTML5 Code for Halting the DOM-Based XSS Vulnerabilities in Cloud. *International Journal of Cloud Applications and Computing (IJCAC)*, 7(1):1–31, January 2017.

- [67] Brij Gupta, Dharma P. Agrawal, Shingo Yamaguchi, and Manish Gupta, editors. *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*. Advances in Information Security, Privacy, and Ethics. IGI Global, 2016.
- [68] T. Hall, S. Beecham, D. Bowes, D. Gray, and S. Counsell. A Systematic Literature Review on Fault Prediction Performance in Software Engineering. *IEEE Transactions on Software Engineering*, 38(6):1276–1304, November 2012.
- [69] Paul’t Hart. Irving l. janis’ victims of groupthink. *Political Psychology*, pages 247–278, 1991.
- [70] Ted Hedesstrom and Edgar A Whitley. What is meant by tacit knowledge? towards a better understanding of the shape of actions. In *ECIS*, pages 46–51, 2000.
- [71] Tejaswini Herath and H. Raghav Rao. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2):106–125, 2009.
- [72] Alan R Hevner, Salvatore T March, Jinsoo Park, and Sudha Ram. Design science in information systems research. *MIS quarterly*, pages 75–105, 2004.
- [73] Michael Hind, Sameep Mehta, Aleksandra Mojsilovic, Ravi Nair, Karthikeyan Natesan Ramamurthy, Alexandra Olteanu, and Kush R Varshney. Increasing trust in ai services through supplier’s declarations of conformity. *arXiv preprint arXiv:1808.07261*, 18:2813–2869, 2018.
- [74] Knut Hinkelmann, Aurna Gerber, Dimitris Karagiannis, Barbara Thoenssen, Alta van der Merwe, and Robert Woitsch. A new paradigm for the continuous alignment of business and IT: Combining enterprise architecture modelling and enterprise ontology. *Computers in Industry*, 79:77–86, June 2016.

- [75] L. Hong and S. E. Page. Groups of diverse problem solvers can outperform groups of high-ability problem solvers. *Proceedings of the National Academy of Sciences*, 101(46):16385–16389, November 2004.
- [76] Michael Hopmere, Lynn Crawford, and Michael S Harré. Proactively monitoring large project portfolios. *Project Management Journal*, 51(6):656–669, 2020.
- [77] Douglas W Hubbard. *The failure of risk management: Why it's broken and how to fix it*. John Wiley & Sons, 2020.
- [78] Maria-Eugenia Iacob and Henk Jonkers. Quantitative analysis of enterprise architectures. In *Interoperability of Enterprise Software and Applications*, pages 239–252. Springer, 2006.
- [79] Hajar Iguer, Hicham Medromi, Adil Sayouti, Soukaina Elhasnaoui, and Sophia Faris. The Impact of Cyber Security Issues on Businesses and Governments: A Framework for Implementing a Cyber Security Plan. pages 316–321. IEEE, August 2014.
- [80] Joint Task Force Transformation Initiative et al. Nist special publication 800-39. *Managing Information Security Risk, Organization, Mission and Information System Review*, 2011.
- [81] Zafar Jafarov. Architecture of an intelligent system for information security management. In *Application of Information and Communication Technologies (AICT), 2013 7th International Conference on*, pages 1–3. IEEE, 2013.
- [82] Irving L Janis. Groupthink. *Psychology today*, 5(6):43–46, 1971.
- [83] Allen C Johnston, Merrill Warkentin, Maranda McBride, and Lemuria Carter. Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems*, 25(3):231–251, 2016.

- [84] Pál Michelberger Jr and Csaba Lábodi. After Information Security – Before a Paradigm Change (A Complex Enterprise Security Model). *Acta Polytechnica Hungarica*, 9(4):17, 2012.
- [85] Kam Jugdev and Janice Thomas. 2002 student paper award winner: Project management maturity models: The silver bullets of competitive advantage? *Project management journal*, 33(4):4–14, 2002.
- [86] Daniel Kahneman. *Thinking, fast and slow*. Macmillan, 2011.
- [87] Daniel Kahneman and Amos Tversky. Intuitive prediction: Biases and corrective procedures. Technical report, Decisions and Designs Inc Mclean Va, 1977.
- [88] Stephen Kaisler and Frank Armour. 15 years of enterprise architecting at hicc: Revisiting the critical problems. In *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.
- [89] Stephen H. Kaisler, Frank Armour, and Michael Valivullah. Enterprise architecting: Critical problems. In *System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on*, pages 224b–224b. IEEE, 2005.
- [90] Staffs Keele. Guidelines for performing systematic literature reviews in software engineering. In *Technical report, Ver. 2.3 EBSE Technical Report. EBSE*. sn, 2007.
- [91] Florian Kerschbaum. Building A Privacy-Preserving Benchmarking Enterprise System. *Enterprise Information Systems*, page 15.
- [92] Nik Zulkarnaen Khidzir, Azlinah Mohamed, and Noor Habibah Arshad. Information security risk factors: Critical threats vulnerabilities in ICT outsourcing. In *Information Retrieval & Knowledge Management, (CAMP), 2010 International Conference on*, pages 194–199. IEEE, 2010.

- [93] Mohammad Khoshgoftar and Omar Osman. Comparison of maturity models. In *2009 2nd IEEE International Conference on Computer Science and Information Technology*, pages 297–301, Beijing, China, 2009. IEEE.
- [94] Geir Kirkebøen. Decision Behaviour- Improving Expert Judgement. In Terry M. Williams, Knut Samset, and Kjell J. Sunnevåg, editors, *Making Essential Choices with Scant Information*, pages 169–194. Palgrave Macmillan UK, London, 2009.
- [95] Norbert Koppenhagen, Oliver Gaß, and Benjamin Müller. Design science research in action-anatomy of success critical activities for rigor and relevance. 2012. University of Mannheim.
- [96] Janne J. Korhonen, James Lapalme, Doug McDavid, and Asif Q. Gill. Adaptive Enterprise Architecture for the Future: Towards a Reconceptualization of EA. In *2016 IEEE 18th Conference on Business Informatics (CBI)*, pages 272–281, Paris, France, August 2016. IEEE.
- [97] Svyatoslav Kotusev. Fake and real tools for enterprise architecture: The zachman framework and business capability model. *Enterprise Architecture Professional Journal*, pages 1–14, 2019.
- [98] Svyatoslav Kotusev and Sherah Kurnia. The theoretical basis of enterprise architecture: A critical review and taxonomy of relevant theories. *Journal of Information Technology*, page 026839622097787, December 2020.
- [99] Svyatoslav Kotusev, Mohini Singh, and Ian Storey. Investigating the usage of enterprise architecture artifacts. 2015.
- [100] Alex Kozinski. What I ate for breakfast and other mysteries of judicial decision making. *Loy. LAL Rev.*, 26:993, 1992.
- [101] Sherah Kurnia, Svyatoslav Kotusev, Graeme Shanks, Rod Dilnutt, and Simon Milton. Stakeholder engagement in enterprise architecture prac-

- tice: What inhibitors are there? *Information and Software Technology*, 134:106536, 2021.
- [102] Vincent Lalanne, Manuel Munier, and Alban Gabillon. Information security risk management in a world of services. In *2013 International Conference on Social Computing*, pages 586–593. IEEE, 2013.
- [103] Thomas Lechler, Susanne Wetzel, and Richard Jankowski. Identifying and evaluating the threat of transitive information leakage in healthcare systems. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, pages 1–10. IEEE, 2011.
- [104] MG Lee. Securing the human to protect the system: Human factors in cyber security. In *7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012*, pages 1–5. IET, 2012.
- [105] Jianzhong Li, Chuying Yu, B. B. Gupta, and Xuechang Ren. Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition. *Multimedia Tools and Applications*, 77(4):4545–4561, February 2018.
- [106] Xu Li and Liu Hongyan. Proposal for information security architecture based on a company. In *Communication Systems, Networks and Applications (ICCSNA), 2010 Second International Conference on*, volume 1, pages 17–20. IEEE, 2010.
- [107] Jeffrey K Liker. *Toyota way: 14 management principles from the world’s greatest manufacturer*. McGraw-Hill Education, 2004.
- [108] Rensis Likert. A technique for the measurement of attitudes. *Archives of psychology*, 1932.
- [109] Paul Loft, Ying He, Helge Janicke, and Isabel Wagner. Dying of a hundred good symptoms: why good security can still fail - a literature review and analysis. *Enterprise Information Systems*, pages 1–26, April 2019.

- [110] Jan Löhe and Christine Legner. Overcoming implementation challenges in enterprise architecture management: a design theory for architecture-driven it management (adrima). *Information Systems and e-Business Management*, 12(1):101–137, 2014.
- [111] Isabel Lopes and Pedro Oliveira. Understanding information security culture: a survey in small and medium sized enterprises. In *New Perspectives in Information Systems and Technologies, Volume 1*, pages 277–286. Springer, 2014.
- [112] Martin Luethi and Gerhard F. Knolmayer. Security in health information systems: an exploratory comparison of US and swiss hospitals. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on*, pages 1–10. IEEE, 2009.
- [113] J. Madison. Agile Architecture Interactions. *IEEE Software*, 27(2):41–48, March 2010.
- [114] Jo Malcolmson. What is security culture? Does it differ in content from general organisational culture? In *Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on*, pages 361–366. IEEE, 2009.
- [115] Nigel Martin and John Rice. Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security*, 30(8):803–814, November 2011.
- [116] Adnan Masood. Cyber security for service oriented architectures in a Web 2.0 world: an overview of SOA vulnerabilities in financial services. In *Technologies for Homeland Security (HST), 2013 IEEE International Conference on*, pages 1–6. IEEE, 2013.
- [117] Michelle McClintock, Katrina Falkner, Claudia Szabo, and Yuval Yarom. Enterprise security architecture: Mythology or methodology? In *ICEIS (2)*, pages 679–689, 2020.

- [118] Rebecca Mears and Kieran Sweeney. A preliminary study of the decision-making process within general practice. *Family Practice*, 17(5):428–429, 2000.
- [119] Pál Michelberger Jr and Csaba Lábodi. After information security—before a paradigm change (a complex enterprise security model). *Acta Polytechnica Hungarica*, 9(4):101–116, 2012.
- [120] Dana M. Milanovich, James E. Driskell, Renee J. Stout, and Eduardo Salas. Status and cockpit dynamics: A review and empirical study. *Group Dynamics: Theory, Research, and Practice*, 2(3):155–167, 1998.
- [121] Mavuto M Mukaka. A guide to appropriate use of correlation coefficient in medical research. *Malawi medical journal*, 24(3):69–71, 2012.
- [122] N. R. Mukundan and L. Prakash Sai. Perceived information security of internal users in Indian IT services industry. *Information Technology and Management*, 15(1):1–8, March 2014.
- [123] Jeryl L. Mumpower and Thomas R. Stewart. Expert Judgement and Expert Disagreement. *Thinking & Reasoning*, 2(2-3):191–212, July 1996.
- [124] Adrian Munteanu, Doina Fotache, and Octavian Dospinescu. Information Systems Security Risk Assessment: Harmonization with International Accounting Standards. pages 1111–1117. IEEE, 2008.
- [125] U. S. Government Accountability Office. Aviation Safety: FAA Efforts Have Improved Safety, but Challenges Remain in Key Areas. (GAO-13-442T), April 2013.
- [126] Eijiroh Ohki, Yonosuke Harada, Shuji Kawaguchi, Tetsuo Shiozaki, and Tetsuyuki Kagaya. Information security governance framework. In *Proceedings of the first ACM workshop on Information security governance*, pages 1–6. ACM, 2009.

- [127] Jim Ollhoff and Michael Walcheski. Making the jump to systems thinking, 2006. The Systems Thinker.
- [128] Prince Onabajo, Pavol Zavorsky, Dale Lindskog, and Ron Ruhl. The study of civil litigation in data storage environment. In *Internet Security (WorldCIS), 2012 World Congress on*, pages 224–230. IEEE, 2012.
- [129] Scott Page. *The diversity bonus*. Princeton University Press, 2019.
- [130] Scott E Page. Making the difference: Applying a logic of diversity. *Academy of Management Perspectives*, 21(4):6–20, 2007.
- [131] Sangseo Park, Atif Ahmad, and Anthonie B. Ruighaver. Factors influencing the implementation of information systems security strategies in organizations. In *Information Science and Applications (ICISA), 2010 International Conference on*, pages 1–6. IEEE, 2010.
- [132] Ken Peffers, Tuure Tuunanen, Marcus A Rothenberger, and Samir Chatterjee. A design science research methodology for information systems research. *Journal of management information systems*, 24(3):45–77, 2007.
- [133] Marcus Pendleton, Richard Garcia-Lebron, Jin-Hee Cho, and Shouhuai Xu. A survey on systems security metrics. *ACM Computing Surveys (CSUR)*, 49(4):1–35, 2016.
- [134] Marcus Pendleton, Richard Garcia-Lebron, Jin-Hee Cho, and Shouhuai Xu. A Survey on Systems Security Metrics. *ACM Computing Surveys*, 49(4):1–35, December 2016.
- [135] Karlene Kassner Petitt. *Safety culture, training, understanding, aviation passion: The impact on manual flight and operational performance*. Embry-Riddle Aeronautical University, 2019.
- [136] Robert M. Polstra III. A case study on how to manage the theft of information. In *Proceedings of the 2nd annual conference on Information security curriculum development*, pages 135–138. ACM, 2005.

- [137] Jan Pries-Heje and Richard Baskerville. The design theory nexus. *MIS quarterly*, pages 731–755, 2008.
- [138] Ira Puspitasari. Stakeholder’s expected value of enterprise architecture: An enterprise architecture solution based on stakeholder perspective. In *2016 IEEE 14th International Conference on Software Engineering Research, Management and Applications (SERA)*, pages 243–248. IEEE, 2016.
- [139] Jackie Rees, Subhajyoti Bandyopadhyay, and Eugene H Spafford. Pfires: A policy framework for information security. *Communications of the ACM*, 46(7):101–106, 2003.
- [140] Cumbal Renato and Narváez María. Technologies’ application, rules, and challenges of information security on information and communication technologies. In *2015 Asia-Pacific Conference on Computer Aided System Engineering*, pages 380–386. IEEE, 2015.
- [141] Jeanne W. Ross, Peter Weill, and David C. Robertson. *Enterprise Architecture As Strategy: Creating a Foundation for Business Execution*. Harvard Business School Press, Boston, Mass, August 2006.
- [142] Souad Sadki and Hanan El Bakkali. Towards controlled-privacy in e-health: A comparative study. In *Multimedia Computing and Systems (ICMCS), 2014 International Conference on*, pages 674–679. IEEE, 2014.
- [143] Hamid M Salim. *Cyber safety: A systems thinking and systems theory approach to managing cyber security risks*. PhD thesis, Massachusetts Institute of Technology, 2014.
- [144] Vasileios Samaras, Semir Daskapan, Rizwan Ahmad, and Sayan Kumar Ray. An enterprise security architecture for accessing saas cloud services with byod. In *2014 Australasian Telecommunication Networks and Applications Conference (ATNAC)*, pages 129–134. IEEE, 2014.

- [145] Stefan Savage and Fred B Schneider. Security is not a commodity: The road forward for cybersecurity research. *Retrieved May*, 31:2010, 2009.
- [146] Reijo M Savola and Petri Heinonen. A visualization and modeling tool for security metrics and measurements management. In *2011 Information Security for South Africa*, pages 1–8. IEEE, 2011.
- [147] Christina Schmidt, Fabienne Collette, Christian Cajochen, and Philippe Peigneux. A time to think: circadian rhythms in human cognition. *Cognitive neuropsychology*, 24(7):755–789, 2007.
- [148] Michael Scriven. The logic and methodology of checklists. 2000. Cite-seer.
- [149] Ravi Sen and Sharad Borle. Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems*, 32(2):314–341, April 2015.
- [150] Hanifa Shah and Mohamed El Kourdi. Frameworks for enterprise architecture. *IT Professional*, 9(5):36–41, 2007.
- [151] Riaz A. Shaikh, Saeed Rajput, S. M. H. Zaidi, and Kashif Sharif. Comparative analysis and design philosophy of next generation unified enterprise application security. In *Emerging Technologies, 2005. Proceedings of the IEEE Symposium on*, pages 517–524. IEEE, 2005.
- [152] Marzieh Shariati, Faezeh Bahmani, and Fereidoon Shams. Enterprise information security, a review of architectures and frameworks from interoperability perspective. *Procedia Computer Science*, 3:537–543, 2011.
- [153] Emad Sherif, Steven Furnell, and Nathan Clarke. Awareness, behaviour and culture: The ABC in cultivating security compliance. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 90–94. IEEE, 2015.

- [154] John Sherwood, Andrew Clark, and David Lynas. *Enterprise Security Architecture: A Business-Driven Approach*. CRC Press, San Francisco, 1 edition edition, November 2005.
- [155] Jordan Shropshire. A canonical analysis of intentional information security breaches by insiders. *Information Management & Computer Security*, 17(4):296–310, October 2009.
- [156] Ang Boon Sin, Suhaiza Zailani, Mohammad Iranmanesh, and T Ramayah. Structural equation modelling on knowledge creation in six sigma dmaic project and its impact on organizational performance. *International Journal of Production Economics*, 168:105–117, 2015.
- [157] Anand Singh and David Lilja. Improving risk assessment methodology: a statistical design of experiments approach. In *Proceedings of the 2nd international conference on Security of information and networks*, pages 21–29. ACM, 2009.
- [158] Mikko Siponen and Robert Willison. Information security management standards: Problems and solutions. *Information & management*, 46(5):267–270, 2009.
- [159] Rolf Skjong and Benedikte H Wentworth. Expert Judgment and Risk Perception. page 9.
- [160] Bill Smith. Six-sigma design (quality control). *IEEE spectrum*, 30(9):43–47, 1993.
- [161] Ronald D Snee. Lean six sigma—getting better all the time. *International Journal of Lean Six Sigma*, 2010.
- [162] Teodor Sommestad, Mathias Ekstedt, and Peter Johnson. Cyber security risks assessment with bayesian defense graphs and architectural models. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on*, pages 1–10. IEEE, 2009.

- [163] Zahoor Ahmed Soomro, Mahmood Hussain Shah, and Javed Ahmed. Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2):215–225, April 2016.
- [164] Janine L Spears. A holistic risk analysis method for identifying information security risks. In *Working Conference on Integrity and Internal Control in Information Systems*, pages 185–202. Springer, 2004.
- [165] Bernd Carsten Stahl, Job Timmermans, and Brent Daniel Mittelstadt. The Ethics of Computing: A Survey of the Computing-Oriented Literature. *ACM Computing Surveys*, 48(4):1–38, February 2016.
- [166] Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, and Brij Gupta. Secure integration of IoT and Cloud Computing. *Future Generation Computer Systems*, 78:964–975, January 2018.
- [167] Jianguang Sun and Yan Chen. Intelligent enterprise information security architecture based on service oriented architecture. In *2008 International Seminar on Future Information Technology and Management Engineering*, pages 196–200. IEEE, 2008.
- [168] Malini D. Sur, Nancy Schindler, Puneet Singh, Peter Angelos, and Alexander Langerman. Young surgeons on speaking up: when and how surgical trainees voice concerns about supervisors’ clinical decisions. *The American Journal of Surgery*, 211(2):437–444, February 2016.
- [169] A. Sviridov, V. Bobkov, D. Bobrikov, and A. Balashov. The Concept of Information Security in the Process Control System. In *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pages 2162–2164, January 2019.
- [170] Maryam Tahajod, Azadeh Iranmehr, and Mohammad Reza Darajeh. A roadmap to develop enterprise security architecture. In *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, pages 1–5. IEEE, 2009.

- [171] Hideyuki Tanaka. Quantitative analysis of information security interdependency between industrial sectors. In *Proceedings of the 2009 3rd International Symposium on Empirical Software Engineering and Measurement*, pages 574–583. IEEE Computer Society, 2009.
- [172] Heli Tervo and Timo Wiander. Sweet dreams and rude awakening-critical infrastructure’s focal it-related incidents. In *2010 43rd Hawaii International Conference on System Sciences*, pages 1–8. IEEE, 2010.
- [173] The Australian National University, Shirley Gregor, Alan R. Hevner, and University of South Florida. Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*, 37(2):337–355, February 2013.
- [174] Aggeliki Tsohou, Maria Karyda, Spyros Kokolakis, and Evangelos Kiountouzis. Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, 24(1):38–58, 2015.
- [175] Jonathan Vallerand, James Lapalme, and Alexandre Moïse. Analysing enterprise architecture maturity models: a learning perspective. *Enterprise Information Systems*, 11(6):859–883, July 2017.
- [176] Corinna Vehlow, Michael Burch, Hansjorg Schmauder, and Daniel Weiskopf. Radial layered matrix visualization of dynamic graphs. In *2013 17th International Conference on Information Visualisation*, pages 51–58. IEEE, 2013.
- [177] John Venable, Jan Pries-Heje, and Richard Baskerville. A comprehensive framework for evaluation in design science research. In *International Conference on Design Science Research in Information Systems*, pages 423–438. Springer, 2012.
- [178] Nesren Waly, Rana Tassabehji, and Mumtaz Kamala. Improving organisational information security management: The impact of training and awareness. In *2012 IEEE 14th International Conference on*

- High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems*, pages 1270–1275. IEEE, 2012.
- [179] Hui Wang, Heli Xu, Bibo Lu, and Zihao Shen. Research on security architecture for defending insider threat. In *2009 Fifth International Conference on Information Assurance and Security*, volume 2, pages 30–33. IEEE, 2009.
- [180] Michael E. Whitman and Herbert J. Mattord. *Principles of information security*. Course Technology, Boston, MA, 4th ed edition, 2012.
- [181] Ping Xiong, Lefeng Zhang, and Tianqing Zhu. Reward-based spatial crowdsourcing with differential privacy preservation. *Enterprise Information Systems*, 11(10):1500–1517, November 2017.
- [182] Jing Yang, Matthew O Ward, and Elke A Rundensteiner. Interring: An interactive tool for visually navigating and manipulating hierarchical structures. In *IEEE Symposium on Information Visualization, 2002. INFOVIS 2002.*, pages 77–84. IEEE, 2002.
- [183] Dong-Young Yoo, Wan S. Yi, Gang Shin Lee, and Jin Young Choi. A method of measuring the propagation of damage to information communication system. In *Software Engineering and Data Mining (SEDM), 2010 2nd International Conference on*, pages 192–196. IEEE, 2010.
- [184] John A Zachman. A framework for information systems architecture. *IBM systems journal*, 26(3):276–292, 1987.
- [185] Xuan Zhang, Nattapong Wuwong, Hao Li, and Xuejie Zhang. Information security risk management framework for the cloud computing environments. In *2010 10th IEEE international conference on computer and information technology*, pages 1328–1334. IEEE, 2010.

- [186] Zhenjiang Zhang, Xiaoni Wang, Lorna Uden, Peng Zhang, and Yingsi Zhao. e-DMDAV: A new privacy preserving algorithm for wearable enterprise information systems. *Enterprise Information Systems*, 12(4):492–504, April 2018.
- [187] Gang Zhao. Holistic framework of security management for cloud service providers. In *Industrial Informatics (INDIN), 2012 10th IEEE International Conference on*, pages 852–856. IEEE, 2012.
- [188] Žužek, T.; Gosar, Ž.; Kušar, J.; Berlec, T. Adopting Agile Project Management Practices in Non-Software SMEs: A Case Study of a Slovenian Medium-Sized Manufacturing Company. *Sustainability 2020*, 2020.

Appendix A

Node Analysis Table

Key to headings

- Dom Domain identified for the node
Src Count of source files for coding of the node
Ref Count of references overall for the node
F r Correlation coefficient value of node to Failure references
S r Correlation coefficient value of node to Success references
r \geq 0.3 Count of correlation values with other nodes that were 0.3 or above
Inf Influence values calculated from the full (non-rounded) r values

Name of Node	Dom	Src	Ref	F r	S r	r \geq 0.3	Inf
Accidental	HF	2	6	0.65	0.00	13	8.48
Accountability	HF	9	19	0.30	0.51	21	10.79
Accuracy	SG	2	3	0.58	0.21	7	4.03
Agility	TI	4	6	0.00	0.60	6	3.59
Application hacking	HF	8	12	0.65	0.00	9	5.84
Architecture	EA	17	30	0.08	0.67	15	10.07
Asset Management	IA	26	46	0.36	0.54	20	10.81
Automation	BP	3	3	0.00	0.55	4	2.21
Business Continuity	BP	8	12	0.33	0.44	19	8.29
Business Process	BP	23	55	0.56	0.40	30	16.77
Business-driven	SG	27	48	0.49	0.44	34	16.71
Communication	HF	15	25	0.27	0.56	21	11.84
Compartmentalisation	TI	4	5	0.42	0.24	7	2.91

Name of Node	Dom	Src	Ref	F r	S r	r \geq 0.3	Inf
Complexity	TI	16	33	0.60	0.21	18	10.72
Configuration	TI	15	19	0.39	0.29	9	3.52
Continuous improvement	SG	13	19	0.20	0.62	19	11.75
Controls operation	HF	8	23	0.58	0.27	21	12.09
Controls selection	TI	22	51	0.43	0.50	34	17.12
Culture	HF	8	25	0.25	0.57	18	10.19
Dependency	BP	2	4	0.59	0.00	3	1.76
Disaster Recovery	TI	3	4	0.59	0.00	6	3.53
Documentation	HF	3	5	0.35	0.28	8	2.80
Economics	EF	24	45	0.57	0.29	26	14.88
Enterprise structure	SG	4	7	0.40	0.29	13	5.18
External to secure network	IA	13	19	0.68	0.00	14	9.51
Flexibility	TI	4	4	0.27	0.45	8	3.57
Fragmentation	TI	4	11	0.66	0.00	9	5.94
Framework	EA	2	2	0.33	0.38	2	0.76
Governance	SG	17	36	0.28	0.56	23	12.83
Holistic perspective	EA	23	34	0.15	0.63	13	8.25
Human Factors	HF	21	104	0.64	0.40	31	19.84
Information Sharing	EF	15	24	0.63	0.08	17	10.66
Integration	TI	12	17	0.34	0.41	12	4.93
Internal Threat	HF	18	38	0.71	0.10	18	12.80
Interoperability	BP	4	8	0.62	0.07	13	8.00
Knowledge	HF	26	69	0.50	0.48	33	16.48
Least privilege	HF	6	8	0.40	0.24	7	2.79
Managed	MI	21	35	0.38	0.52	31	15.98
Management assurance	MI	2	6	0.51	0.21	8	4.05
Management influence	MI	14	30	0.39	0.48	25	12.05
Monitoring	MI	17	32	0.21	0.61	25	15.33
multiple vulnerabilities	TI	7	14	0.52	0.19	13	6.70
New technology	TI	25	38	0.54	0.31	26	14.08
Non-digital	IA	2	5	0.46	0.08	4	1.86
Openness	HF	4	4	0.28	0.28	6	*
Performance degradation	TI	2	3	0.64	0.00	3	1.91
Persuasion	MI	3	9	0.18	0.50	14	7.03
Predictability	EF	1	1	0.48	0.00	2	0.97
Redundancy	TI	3	3	0.43	0.19	4	1.72
Regulation	EF	11	20	0.38	0.34	16	6.05
Reliability	TI	5	5	0.51	0.10	9	4.57
Risk Management	SG	37	74	0.33	0.64	25	15.95

Name of Node	Dom	Src	Ref	F r	S r	$r \geq 0.3$	Inf
Scalability	TI	1	1	0.00	0.37	3	1.10
Security resources	SG	17	29	0.39	0.42	19	8.04
Security Strategy	SG	8	18	0.43	0.38	19	8.17
Social environment	HF	3	10	0.23	0.52	14	7.31
Standardisation	TI	10	22	0.16	0.62	22	13.62
Supervision	MI	10	14	0.26	0.49	17	8.33
Systems perspective	BP	1	1	0.00	0.50	1	0.50
Systems Thinking	BP	6	10	0.16	0.55	13	7.21
Technology Assurance	TI	15	20	0.32	0.40	16	6.43
Third-party relationship	EF	20	41	0.62	0.18	21	13.02
Timescales	SG	11	16	0.61	0.14	17	10.41
Trust	HF	11	15	0.20	0.53	11	5.79
Uncertainty	EF	4	9	0.64	0.00	13	8.29

Table A.2: Node Analysis

*Both correlation values are too low for inclusion.

Note that calculations for *influence* in this table are based on the full correlation values (not the rounded values shown here).

Appendix B

Correlation values for sectors

Node	Private	Public	Strongest
Accountability	0.20	0.15	0.20
Application hacking	0.33	0.00	0.33
Architecture	0.15	0.09	0.15
Complexity	0.30	0.18	0.30
Controls operation	0.00	0.16	0.16
Controls selection	0.00	0.15	0.15
Disaster Recovery	0.44	0.00	0.44
Economics	0.43	0.33	0.43
Holistic perspective	0.19	0.00	0.19
Human Factors	0.24	0.14	0.24
Integration	0.24	0.00	0.24
Internal Threat	0.28	0.18	0.28
Knowledge	0.25	0.14	0.25
Managed	0.22	0.00	0.22
Management influence	0.22	0.14	0.22
Monitoring	0.16	0.00	0.16
Regulation	0.32	0.31	0.32
Risk Management	0.28	0.00	0.28
Security resources	0.25	0.16	0.25
Security Strategy	0.35	0.00	0.35
Standardisation	0.00	0.13	0.13
Technology Assurance	0.00	0.28	0.28

Node	Private	Public	Strongest
Third-party relationship	0.27	0.18	0.27
Trust	0.21	0.18	0.21

Table B.2: Sector Node Correlations

Appendix C

Analysis of strong pairwise node correlation

Key for table C.2

- Dm1 and Dm2 = the domains included in the pairwise comparison.
- Node1 and Node2 = the nodes featured in the correlation.
- r = correlation coefficient.
- The *italicized* text summarizes the literature references identified in the coding of the literature review.
- The figures in square brackets denote the relevant CAESAR8 level, e.g., [#].

Item	Dm1	Node1	Dm2	Node2	r
(1)	IA	Asset Management	SG	Risk Management	0.63
		<i>Consider latest threats; focus on business impact; maintain enterprise perspective; keep current; monitor; define for developers [3]</i>			
(2)	IA	External to se- cure network	HF	Application Hacking	0.51

Item	Dm1	Node1	Dm2	Node2	r
<i>Consider access to third parties; consider external data [2]</i>					
(3)	IA	External to se- cure network	TI	Disaster Recovery	0.51
<i>Difficult to prevent breaches so plan for them; act decisively when breaches occur [3]</i>					
(4)	IA	External to se- cure network	EF	Information Shar- ing	0.69
<i>Network boundary data at risk, so needs good architecture; be aware of data leaving the organization's network; sharing personal data must be legal; linking networks exposes risks to one another [3]</i>					
(5)	IA	External to se- cure network	IA	Non-digital	0.74
<i>Loss of control of data leaving the network (people and paper) [3]</i>					
(6)	EF	Economics	TI	Flexibility	0.54
<i>Align security programs to business needs and contribute to the bottom line. Adapt to new risks and focus on the long term [stakeholders know long term] [1,3]</i>					
(7)	EF	Economics	TI	Reliability	0.53
<i>Nearly half budget spent on h/w and s/w that may introduce more vulnerabilities than benefit. A reliable, scalable architecture is benefit [4]</i>					
(8)	EF	Third Party Rela- tionship	SG	Enterprise Struc- ture	0.54
<i>Disharmony in company objectives and contractor values. Weakness of structures. Establish controls upfront - e.g. access and audit [2]</i>					
(9)	EF	Third Party Rela- tionship	IA	External to net- work	0.56
<i>Business processes involving data often transcend company bound-aries. Companies may have lost control of their data. Intruders may attack weaker remote points [1]</i>					
(10)	EF	Third Party Rela- tionship	EF	Information Shar- ing	0.63
<i>Poor control of data ownership leads to unauthorized disclosure. Data aggregation through sequence of exchanges increases risk. Retaining data post transaction increases risk [1, 4]</i>					
(11)	EF	Information Shar- ing	TI	Fragmentation	0.55

Item	Dm1	Node1	Dm2	Node2	r	
<i>System interfaces (particularly legacy) are developed bespoke and point-to-point lacking security standards and architecture, e.g. authentication and audit. New data pools created to support new processes. New components often developed for new tasks as legacy systems have poor documentation and too expensive to change. Data can become hidden [1,4,5]</i>						
(12)	EF	Information Shar-	BP	Interoperability	0.59	
ing						
<i>Similar to 'fragmentation' node above. EISA supports balancing security and interoperability [5]</i>						
(13)	EF	Uncertainty	TI	New Technology	0.51	
<i>Increase in technology leads to greater uncertainty. Pace of change can mismatch security and business strategy. More sophisticated technology leads to greater security risks, so technology can both support and hinder security. Pace of deployment hinders identification of security vulnerabilities [2]</i>						
(14)	EF	Uncertainty	SG	Timescales	0.51	
<i>Technology deployed without sufficient time for analysis of security vulnerabilities [2]</i>						
(15)	EF	Uncertainty	EF	Predictability	0.77	
<i>Standardization improves security by improving predictability as uncertainty about threats increases [5]</i>						
(16)	TI	Controls	Selec-	EA	Framework	0.57
tion						
<i>Use of frameworks and practical tools help to prevent breaches [4]</i>						
(17)	TI	Controls	Selec-	TI	Performance	0.64
tion						
Degradation						
<i>A badly implemented control can impact another control - e.g. poor authentication harms access control measures [4,5]</i>						
(18)	TI	Controls	Selec-	SG	Risk	0.51
tion						
Management						

Item	Dm1	Node1	Dm2	Node2	r
<i>Information security can become a barrier; accept failure and prepare by having systems and trained personnel to recover. Non-IT personnel must be involved in evaluating business processes to provide information assurance. Common work attitude drives security culture - consider management and co-workers. Most businesses do not know how they actually operate - therefore miss-matched technology can create vulnerabilities. Understand information flows. Common security incidents are insider errors. Security controls must consider users and how they work [4]</i>					
(25)	BP	Interoperability	TI	Fragmentation	0.71
<i>Connecting systems can result in multiple data pools with point-to-point connections. Vendors do not implement security interoperability due to lack of standards [4]</i>					
(26)	EA	Architecture	BP	Automation	0.50
<i>Architecture should be easy to maintain - administration should not be challenging. Know its strengths and weaknesses [5]</i>					
(27)	EA	Architecture	EA	Holistic Perspective	0.57
<i>Contribution of each group of security controls is important for the performance of the organization's security framework. A multi-pronged action is necessary to cover technical and other controls (people, processes, and business goals that support the technology). Maintain organizational context. A model should enforce defining elements and linking to a framework, which should contain existing elements [2,3,4]</i>					
(28)	SG	Business-driven	SG	Timescales	0.51
<i>Dynamic security strategies keep pace with the business; fluid work practices that maximize speed of delivery but lack security standards and procedures can lead to failure of information security. Business and economics can determine security decisions. Security strategies must keep pace with business change and observe changes in vulnerabilities [2,3,4]</i>					
(29)	SG	Risk Management	SG	Accuracy	0.53
<i>As organizations become large and complex, data collected for risk assessments becomes inaccurate, and identifying the attack surface is difficult [3]</i>					
(30)	SG	Risk Management	SG	Flexibility	0.55

Item	Dm1	Node1		Dm2	Node2	r
<i>Security management must allow the business to adapt and prosper and make the organization more resilient. Balance business and technology boundaries so that organizations can respond to business opportunities, regulatory pressures and evolving threats [1,2,4]</i>						
(31)	SG	Risk Management	Manage-	EA	Framework	0.56
<i>Standards only provide a baseline and need to be reinforced by frameworks and practical tools to prevent breaches [4]</i>						
(32)	SG	Governance		MI	Management In-	0.77
<i>fluence</i>						
<i>Support and influence of top management is key. Management need to approach information security in an holistic way. Awareness of top management (in information security) is not being prioritized. "Urgency" prioritized over standard procedures. (Example: development team was fluid and innovative, and meeting business priorities; but lacking discipline, formal procedures and isolated themselves.) Security solution should not be technology alone but management need to understand the business and risks. Security expectation is set from the top. Boss, colleague and computer specialist were all more influential than top management and the security department. A weak understanding of top management's requirements for information security was a possible cause. Company executives need to review and be accountable for information security risks and not consider this as an administrative matter that can be resolved by a bottom-up approach. User will do what they believe is right, so consider this when designing systems. Management should be alerted when their thresholds are breached. [2,3,4]</i>						
(33)	SG	Continuous Improvement	Im-	HF	Communication	0.57
<i>Information security may be a continuous cycle. Simply communicating security documentation (without management influence and monitoring) may not be sufficient to improve security maturity. Implementation of the security strategy must be easy to understand in its entirety (i.e. the whole architecture), and how it effects the environment [4]</i>						
(34)	SG	Continuous Improvement	Im-	HF	Culture	0.57

Item	Dm1	Node1	Dm2	Node2	r
(40)	MI	Monitoring	MI	Managed	0.57
<i>Documented processes allow audit. Ensure that only the minimal information required is stored and regularly check access, to establish trust between entities. All systems should be reviewed for vulnerabilities and patches applied regularly. Lack of unified planning and auditing of security identified in one [incident] case [4,5]</i>					
(41)	MI	Monitoring	MI	Management Assurance	0.50
<i>Monitoring and enforcement is a challenge [4,5]</i>					
(42)	MI	Management Influence	In- HF	Knowledge	0.52
<i>Multi-pronged approach required. Senior management not aware of real priority of security. Business demands taking priority. Reward good performance, and assess effectiveness by measuring how skills are transferred to the workplace. A lack of commitment to responsibilities and incident reporting are key barriers. Positive reinforcement is important. Persuasive strategies help build a good security culture [4]</i>					
(43)	MI	Management Influence	In- HF	Social Environment	0.59
<i>Social environment effects employees attitudes to security. Security strategy fails if it does not address individual values, beliefs and encourages conformity. Management practices and coworker socialization, affect security behavior. (Example: development team created its own isolated, situation-driven culture – high innovation, weak discipline [4])</i>					
(44)	MI	Supervision	MI	Monitoring	0.62
<i>Important to determine security compliance, as self-preservation is priority. Observe employees lives. Regulation/legal can help data keepers to be more vigilant. Technical controls can help security (e.g. encryption) but must be monitored for user compliance. Awareness of monitoring, and the likelihood of sanctions being enforced, positively influence behavior [4,5]</i>					
(45)	MI	Supervision	MI	Persuasion	0.62
<i>Measure user attitude, then influence by personal, social or persuasive strategies. Deterrent efforts should correspond to certainty of sanctions (i.e. a very severe penalty is unlikely to be enforced [4])</i>					
(46)	MI	Supervision	HF	Social Environment	0.66

Item	Dm1	Node1	Dm2	Node2	r
<i>Employee security knowledge can be obtained by training and common work attitude [4]</i>					
(47)	HF	Human Factors	HF	Internal Threat	0.73
<i>Strong controls can limit productivity, but weak controls risk security incidents. Users would share accounts if more convenient and often do work on their home computers. Well-meaning slips are the most common of incidents. Human failure follows predictable patterns. Internal ‘intruders’ may be employed by the company. Insiders do most damage, so need to be targeted for countermeasures. Monitoring users is key to enforcing security. Observing personal issues of staff (e.g. financial, relationships, substance misuse and job changes) should be observed for signs of emotional dissonance. Closer monitoring should be undertaken when issues identified. Assuming that “security is everyone’s responsibility”, may actually mean that it is no one’s responsibility. Making one person responsible, (e.g. CISO) who does not have the capability is ineffective. Suppliers ‘remoting in’ can cause breaches. Loss of devices and accidental disclosure cited. Deliberate breaches can be small in number. BYOD increased risk. Collusion opportunities between internal and external attacker are a threat [4]</i>					
(48)	HF	Human Factors	HF	Knowledge	0.70

Item	Dm1	Node1	Dm2	Node2	r
(51)	HF	Human Factors	HF	Supervision	0.65
<i>Self-preservation is instinctive, information security is not. Factors in employees lives impact behavior. Managers need to listen and show concern for their well-being. Technical controls and procedures should be developed to prevent intentional breaches. Poor motivation causes security failures. Better education, encouragement and commitment helps [4]</i>					
(52)	HF	Knowledge	HF	Documentation	0.66
<i>Poor security documentation can be “catastrophic”. Ensure that employees can actually perform the necessary activities that are needed to comply with policy. Users/employees need to be given the necessary resources to comply [4]</i>					
(53)	HF	Knowledge	HF	Persuasion	0.53
<i>Managers need to pay attention to awareness [4]</i>					
(54)	HF	Knowledge	HF	Social Environment	0.52
<i>Knowledge is influenced by common work attitudes, organizational commitment, and a belief that individuals should replicate the actions of their peers [1,4]</i>					
(55)	HF	Knowledge	EF	Predictability	0.54
<i>Attacks are increasingly unpredictable, so standardization is important to achieving security objectives [5]</i>					
(56)	HF	Internal Threat	TI	Performance Degradation	0.51
<i>Unrefined authentication and authorization procedures can limit productivity, but lax controls defeat security measures [4]</i>					
(57)	HF	Internal Threat	MI	Supervision	0.51
<i>Unsupervised sharing of devices was evident. Balance supervision - caring rather than suspicious. Procedures to manage terminations are needed [4]</i>					
(58)	HF	Controls	Opera- tion	BP Business Process	0.61

Item	Dm1	Node1	Dm2	Node2	r
(64)	HF	Communication	HF	Documentation	0.62
<i>Security documentation is important, but just documenting and communicating security requirements (as opposed to active management) is a low level of maturity [4]</i>					
(65)	HF	Communication	SG	Governance	0.54
<i>Users perceive security requirements differently from management. Management need to know that merely communicating security requirements does not make the organization secure. Attend to risks associated with IT transformations. Whilst security standards increase awareness, intra-departmental communication transcend traditional “information security” domains. Achieving good security is a continuous cycle and needs to be shaped and directed by attention to many factors. Security strategies need to be easy to understand and implemented with known environmental impact. Decentralize decision making capability. Employees need to perceive that their behaviors have a favorable impact on the organization. Security teams need to analyze current security performance [3,4]</i>					
(66)	HF	Communication	HF	Human Factors	0.56
<i>Being forced to publicize security breaches encourages users not to make mistakes. Listen to what employees are saying about themselves and others. Involve non-IT managers in evaluating business processes. Target messages at/to specific employees; make messages engaging; measure awareness. Awareness plus other factors improves culture. Assess the change process. External disclosure lets employees know that external stakeholders are important. Colleagues and bosses are more influential than top management and security departments. Employees may not actually understand organizational expectations [3,4]</i>					
(67)	HF	Communication	HF	Knowledge	0.62
<i>Making employees aware of security matters is a first step to a good security culture. If employees can perceive the benefit to the organization, they are more likely to comply [4]</i>					
(68)	HF	Communication	MI	Monitoring	0.55
<i>Measuring awareness is important for good security culture [4,5]</i>					
(69)	HF	Communication	MI	Persuasion	0.55
<i>Security culture is shaped and directed. Managers need to make sure that employees have the necessary resources to comply with security policy [4]</i>					
(70)	HF	Accountability	SG	Governance	0.50

Item	Dm1	Node1	Dm2	Node2	r
<i>Determine if the people adhere to policies and procedures. Motivation increases learning. Deterrent efforts bring positive results (monitoring and detection [4])</i>					
(76)	HF	Culture	HF	Human Factors	0.63
<i>Human co-operative behavior is the most significant for a good security culture. Minimize chances of human error to improve culture – this is not simple. Motivate good behavior through penalties for breaches. Bad outsource management leads to stress and user error. “Every [security] system is inadequate if there is no security culture shared by the whole staff” [4,5]</i>					
(77)	HF	Culture	HF	Knowledge	0.53
<i>Good security culture may be as simple as making sure that individuals are aware that security matters. Measuring security awareness through organizational change is significant. Staff appraisals are a good vehicle for assessing and reinforcing information security awareness. Peer behavior will influence an individual’s behavior [4]</i>					
(78)	HF	Culture	MI	Management Influence	0.53
<i>Organizational objectives and social values determine the importance of protecting personal information. Good security culture needs to be shaped and directed. It cannot be created. Creating teams focused on deadlines and innovation can create weak discipline, leading to security breaches. Stressful operating environments lead to user error. Managers can improve security compliance by enhancing the security climate [2,3]</i>					
(79)	HF	Culture	MI	Monitoring	0.53
<i>Assess and understand human behavior. Measure security culture [4]</i>					
(80)	HF	Culture	MI	Persuasion	0.61
<i>Culture cannot be created. Persuasive strategies should be sought to improve security behavior [4]</i>					
(81)	HF	Culture	HF	Social Environment	0.59
<i>Social cultural factors influence information security, so organization practices must observe information security. Organizational objectives/culture and social value influence the security culture [4]</i>					
(82)	HF	Accidental	TI	Fragmentation	0.53
<i>IT transformation can lead to security breaches, due to organizational discontinuities [2,3,4]</i>					
(83)	HF	Accidental	HF	Human Factors	0.61

Item	Dm1	Node1	Dm2	Node2	r
<i>Technical mistakes effected other systems due to tight systems coupling. Deadlines forced skipping of testing functions. Complex interconnected systems aggravate security issues. Errors can cause breaches without failure of policy or procedure [2,4,5]</i>					
(84)	HF	Accidental	HF	Internal Threat	0.54
<i>The majority of endpoint breaches are unintentional [4]</i>					
(85)	HF	Accidental	BP	Interoperability	0.52
<i>Mistakes in one system caused major breaches in another coupled system [5]</i>					

Table C.2: Analysis of strongest pairwise nodes

Appendix D

Evaluation Questionnaires

D.1 Questionnaires

The following surveys were created in JISC and presented to volunteers as online questionnaires. Responses were provided in the Likert Scale. Although these are essentially closed questionnaires, every question included an optional open text response to capture any comments.

Pre-evaluation questionnaire

1. Consent Form/Note:

Dear Volunteer

I am a student at De Montfort University in Leicester, researching how organizations might be able to adopt more inclusive enterprise architecture based reviews of Agile business change projects. Our earlier research has analyzed the most significant factors for ensuring the success of information security programs, and has resulted in the design of a novel model that can

quickly and independently combine the reviews of multiple stakeholders. This ensures that organizations are maximizing the benefits of their collective knowledge and experience.

We are now looking to undertake a series of observational field studies to evaluate this new model, which will be conducted in 3 stages:

- A pre-evaluation questionnaire (this questionnaire - about 5 minutes to complete);
- Use of a web app to test the model first-hand (can involve other stakeholders);
- A post-evaluation questionnaire (about 5 minutes to complete).

As a participant in this research, you will not be asked to provide any details about your organization's security. Only anonymous information will be obtained from respondents.

The information that you enter into the questionnaires will be retained in JISC's GDPR compliant online survey tool. Only anonymous summary data and comments will be extracted. Data entered into the web app will be stored in Microsoft's secure Azure cloud service. Use of the web app will be analysed, but only a summary of the analysis, together with any comments, will be extracted for respondents' reports and research documentation purposes. All source data will be kept for no longer than 3 years.

In return for taking part in this research, volunteers will be given a copy of the final results of the evaluation and research; and in addition, will be offered a summary report of their own test results. The direct involvement of other company stakeholders during the evaluation may be important for maximizing the quality of this report, but this aspect is entirely optional.

By providing the information requested on this page, you are agreeing to participate in the research. Your ongoing participation is entirely voluntary and you can elect to be removed from the research at any time. Information that you have already submitted up until that point may already be included in the research, but will remain completely anonymous.

Thank you for helping De Montfort University with the research of CAE-SAR8.

Paul Loft

-New Page-

2. Common challenges faced by information security professionals The following issues may all be important for information security, but how challenging do you think they are for projects currently:

a. Common problems with governance:

(1) Strongly Disagree, (2) Disagree, (3) Neither, (4) Agree, (5) Strongly Agree

Stakeholders not directly engaging with projects

Lack of collaboration across separate teams

Limited understanding of the wider effects of changes

Executive not formally understanding project risks

(Additional free-text information)

b. Common problems with solution design:

(1) Strongly Disagree, (2) Disagree, (3) Neither, (4) Agree, (5) Strongly Agree

Legal compliance reviews not completed for all changes

Security risk management not expressed in a business context

Insufficient rigor applied when working with third parties

Agreed security controls are sometimes omitted

Lack of monitoring of security controls

Project impact on current business processes not fully considered

Lack of clarity over information storage and sharing

Ad hoc deployment of new technology

Not understanding the effect of a new system on all personnel

Testing is not completed adequately

Management unwilling or unable to monitor compliance

(Additional free-text information)

c. Other common security problems:

(1) Strongly Disagree, (2) Disagree, (3) Neither, (4) Agree, (5) Strongly Agree

Time-related pressures are a risk to security

Budget constraints are a risk to security

High workloads are a risk to security

Volume of project changes are a risk to security
Difficult to recruit skilled security personnel
Prioritization of work can be unclear
Disparate security and business risk management methods
Security documentation sometimes inadequate
Lack of adherence to security operating procedures

(Additional free-text information)

-New Page-

3. About you

e. Please tell us your involvement in information security:

My experience is as a full-time information security professional
My involvement in information security is on an ad-hoc basis

(If IS professional, quantify..)

e2. For how many years have you been working in information security?

Less than 5 years
5 years to 10 years
Greater than 10 years
Other

(Additional free-text information)

f. Describe the nature of your work (select all that apply):

(1) Never, (2) Yearly, (3) Monthly, (4) Weekly, (5) Daily

Information Security Governance
Security Strategies
Security Control Frameworks
Organizational Security Policies
Risk Assessment Methodologies
Security Architecture
Software Development
Business Continuity
Legal Compliance (e.g. GDPR)
Operations Security
Incident Management
Audit & Compliance

Security Education

(Additional free-text information)

g. How many ongoing projects do you currently have to support?

Less than 5 projects

5 to 10 projects

More than 10 projects

End.

Volunteers will evaluate the CAESAR8 demonstrator web app between completing pre and post evaluation questionnaires

Post-evaluation questionnaire

1. Your reference

a. Your Evaluation Reference:

b. Your email address:

-New Page-

2. Summary of CAESAR8 evaluation:

b. Please give your view on how CAESAR8 will be able to assist projects:

(1) Strongly Disagree, (2) Disagree, (3) Neither, (4) Agree, (5) Strongly Agree

Ensuring all stakeholders maintain active involvement in projects

Supporting collaboration across separate teams

Maintaining an holistic perspective when agreeing changes

Obtaining senior management acceptance of project issues and risks

Completing legal compliance reviews for all changes

Security risk management is understood in a business context

Applying rigor when working with third parties

Ensuring that agreed security controls are fully implemented

Ensuring security controls will be monitored

Full understanding of how a new system impacts on current business processes

Clarity over information storage and sharing

Ensuring that new technology is implemented in a controlled manner
Understanding how a new system impacts all effected personnel
Ensuring that testing has completed adequately
Ensuring that management will monitor system performance

(Additional free-text information)

c. Please rate these other CAESAR8 characteristics:

(1) Strongly Disagree, (2) Disagree, (3) Neither, (4) Agree, (5) Strongly Agree

The 40 questions covered some key issues to determine success

The 40 questions were easy to understand

It was easy to conduct assessments

Conducting assessments was a quick process

It was valuable to include multiple stakeholders when conducting assessments

The levels (1-5) were meaningful

It was easy to share results with all colleagues and management

It was easy to integrate CAESAR8 with existing DevOps and Project processes

CAESAR8 supports integration with Agile working practices

CAESAR8 assists with the prioritization of work

CAESAR8 will help to maintain essential architecture documentation

(Additional free-text information)

d. The involvement of other stakeholders:

(1) Strongly Disagree, (2) Disagree, (3) Neither, (4) Agree, (5) Strongly Agree

Additional stakeholders could be from other, non-security roles?

The CAESAR8 assessments provided relevant questions for other stakeholders?

The stakeholders could identify performance markers that were relevant to them?

Stakeholders can provide just the responses where they have knowledge/responsibility?

It was easy to combine separate assessments and collaborate on the results?

(Additional free-text information)

-New Page-

e. Please provide details of any project issues that CAESAR8 has helped to uncover:

(Free-text information)

f. Any other comments that you would like to make:

(Free-text information)

g. Would you like to receive a customized report of your findings in relation to the overall assessment:

Yes

No

End.

D.2 Response raw data

The numbering of questions is slightly different when the questionnaires were added to JISC. This is partly due to the preamble included in the official JISC surveys, but the full questions presented are repeated for clarity.

D.2.0.1 Key to response coding

For presentation and analysis purposes, responses have been given the following coding:

Code	Response
5	Strongly Agree
4	Agree
3	Neither
2	Disagree
1	Strongly Disagree

Table D.1: Key to response coding

D.2.1 Participant responses

This chapter includes the responses to the main artifact problem identification and objective questions. To protect the anonymity of respondents, it excludes free-text responses and information about the respondents themselves.

Responses are shown in the order that the questionnaires were completed.

The *Ref* values in square brackets are provided to make it easy to cross reference the 15 common problems identification across pre and post evaluation questionnaires.

D.2.1.1 Pre-evaluation 1 responses

One volunteer did not complete the pre-evaluation questionnaire and therefore did not take part in Eval1.

Ref	S1	S2	T1	B1	T2	B2	S3
<i>Common challenges for information security professionals</i>							
4.	Common problems with governance:						
4.1.	Lack for formal engagement of all project stakeholders						
	5	4	5	5	4	4	4
4.2.	Lack of collaboration across separate teams						
	4	4	5	4	4	5	5
4.3.	Limited understanding of the wider effects of changes						
	5	5	5	4	4	4	4
4.4.	Executive not formally understanding project risks						
	4	5	5	5	4	4	3
5.	Common problems with solution design: Please provide your experience of the following solution design issues						
5.1. [5]	Legal compliance reviews not completed for all changes						

5.2. [6]	4	4	4	4	3	3	3
	Security risk management not expressed in a business context						
	3	2	5	4	4	4	3
5.3. [7]	Insufficient rigor applied when working with third parties						
	3	5	5	4	3	4	4
5.4. [8]	Agreed security controls are sometimes omitted						
	4	4	5	4	3	3	3
5.5. [9]	Lack of monitoring of security controls						
	3	4	5	5	5	4	5
5.6. [10]	Project impact on current business processes not fully considered						
	5	5	4	5	4	4	3
5.7. [11]	Lack of clarity over information storage and sharing						
	5	3	4	4	3	4	3
5.8. [12]	Ad hoc deployment of new technology						
	4	5	5	4	3	5	3
5.9.[13]	Not understanding the effect of a new system on all personnel						
	5	5	5	4	3	5	4
5.10. [14]	Testing is not completed adequately						
	5	4	5	5	5	4	4
5.11. [15]	Management unwilling or unable to monitor compliance						
	4	5	4	4	4	4	4
6.	Other common security problems: Please provide your experience of other security issues						
6.1.	Time-related pressures are a risk to security						
	4	5	5	4	5	4	5
6.2.	Budget constraints are a risk to security						
	4	5	5	5	5	5	4
6.3.	High workloads are a risk to security						
	4	5	4	4	4	4	5
6.4.	Volume of project changes are a risk to security						
	4	5	5	4	4	5	5
6.5.	Difficult to recruit skilled security personnel						
	4	4	4	3	5	3	2
6.6.	Prioritization of work can be unclear						
	5	4	5	4	4	4	4
6.7.	Security documentation sometimes inadequate						
	4	4	4	5	4	3	4
6.8.	Lack of adherence to security operating procedures						
	4	4	5	5	4	3	4

Table D.3: Pre-evaluation 1

D.2.1.2 Post-evaluation 1 responses

Note that one additional volunteer did not respond to the post-evaluation questionnaire for Eval 1.

Ref	S1	T1	S2	B2	S3	B1
3.	Please give your view on how CAESAR8 will be able to assist projects:					
3.1.	Ensuring all stakeholders maintain active involvement in projects					
	4	4	4	5	4	4
3.2.	Supporting collaboration across separate teams					
	4	5	4	5	5	4
3.3.	Maintaining an holistic perspective when agreeing changes					
	4	4	5	5	4	5
3.4.	Obtaining senior management acceptance of project issues and risks					
	5	3	4	5	4	4
3.5.	Completing legal compliance reviews for all changes					
	4	4	4	5	3	4
3.6.	Security risk management is understood in a business context					
	3	4	4	5	4	4
3.7.	Applying rigor when working with third parties					
	3	5	4	5	4	5
3.8.	Ensuring that agreed security controls are fully implemented					
	4	4	3	4	5	5
3.9.	Ensuring security controls will be monitored					
	3	4	4	4	4	5
3.10.	Full understanding of how a new system impacts on current business processes					
	5	4	4	5	4	4
3.11.	Clarity over information storage and sharing					
	4	5	4	5	3	4
3.12.	Ensuring that new technology is implemented in a controlled manner					
	5	4	4	5	5	4
3.13.	Understanding how a new system impacts all effected personnel					

	5	5	4	4	4	5
3.14.	Ensuring that testing has completed adequately					
	4	4	4	4	4	4
3.15.	Ensuring that management will monitor system performance					
	3	3	4	4	3	4
4.	Please rate these other potential CAESAR8 characteristics:					
4.1.	The 40 questions covered some key issues to determine success					
	4	5	4	5	5	4
4.2.	The 40 questions were easy to understand					
	4	5	4	5	4	2
4.3.	It was easy to conduct assessments					
	4	5	4	5	5	4
4.4.	Conducting assessments was a quick process					
	4	5	4	5	5	4
4.5.	It was valuable to include multiple stakeholders when conducting assessments					
	5	5	4	5	5	5
4.6.	The levels (1-5) were meaningful					
	4	5	3	5	4	4
4.7.	It was easy to share results with all colleagues and management					
	4	5	4	5	4	5
4.8.	It was easy to integrate CAESAR8 with existing DevOps and Project processes					
	4	5	3	4	4	4
4.9.	CAESAR8 supports integration with Agile working practices					
	4	5	3	5	4	4
4.10.	CAESAR8 assists with the prioritization of work					
	4	5	4	5	4	3
4.11.	CAESAR8 will help to maintain essential architecture documentation					
	4	5	4	5	4	3
5.	Please rate the involvement of other stakeholders:					
5.1.	Additional stakeholders could be from other, non-security roles					
	5	5	4	5	5	4
5.2.	The CAESAR8 assessments provided relevant questions for other stakeholders					
	4	5	4	4	4	4
5.3.	The stakeholders could identify performance markers that were relevant to them					
	4	5	4	5	4	4
5.4.	Stakeholders can provide just the responses where they have knowledge/responsibility					

	4	5	4	4	5	4
5.5.	It was easy to combine separate assessments and collaborate on the results					
	4	5	4	5	4	5

Table D.5: Post-evaluation 1

D.2.1.3 Pre-evaluation 2 responses

Two volunteers did not complete the pre-evaluation questionnaire and therefore did not take part in Eval2.

Ref	S5	S4	B3	T3	B4	S6	S7
<i>Common challenges for information security professionals</i>							
4.	Common problems with governance:						
4.1.	Lack for formal engagement of all project stakeholders						
	5	4	4	5	4	5	4
4.2.	Lack of collaboration across separate teams						
	5	4	4	4	4	4	4
4.3.	Limited understanding of the wider effects of changes						
	5	4	4	5	4	3	4
4.4.	Executive not formally understanding project risks						
	5	3	3	5	5	4	4
5.	Common problems with solution design: Please provide your experience of the following solution design issues						
5.1. [5]	Legal compliance reviews not completed for all changes						
	5	4	3	5	4	3	3
5.2. [6]	Security risk management not expressed in a business context						
	5	3	2	4	4	2	4
5.3. [7]	Insufficient rigor applied when working with third parties						
	5	5	5	5	5	4	4
5.4. [8]	Agreed security controls are sometimes omitted						
	5	3	4	4	4	5	4
5.5. [9]	Lack of monitoring of security controls						
	5	5	4	5	3	4	4

5.6. [10]	Project impact on current business processes not fully considered	5	5	4	4	5	4	3
5.7. [11]	Lack of clarity over information storage and sharing	5	4	3	4	5	4	3
5.8. [12]	Ad hoc deployment of new technology	5	5	4	4	5	5	3
5.9.[13]	Not understanding the effect of a new system on all personnel	5	5	5	5	5	4	4
5.10. [14]	Testing is not completed adequately	5	4	5	4	4	5	4
5.11. [15]	Management unwilling or unable to monitor compliance	5	5	4	5	5	4	4
6.	Other common security problems: Please provide your experience of other security issues							
6.1.	Time-related pressures are a risk to security	5	4	5	5	4	5	5
6.2.	Budget constraints are a risk to security	5	5	5	4	4	5	5
6.3.	High workloads are a risk to security	5	4	5	5	4	5	4
6.4.	Volume of project changes are a risk to security	4	4	5	4	4	4	4
6.5.	Difficult to recruit skilled security personnel	5	5	5	4	4	4	3
6.6.	Prioritization of work can be unclear	5	4	5	4	4	4	4
6.7.	Security documentation sometimes inadequate	5	5	5	4	4	3	5
6.8.	Lack of adherence to security operating procedures	5	5	5	4	4	5	5

Table D.7: Pre-evaluation 2

D.2.1.4 Post-evaluation 2 responses

Two additional volunteers did not complete the post-evaluation questionnaire and therefore did not complete Eval2.

Ref	B4	T3	S4	S7	S5
3.	Please give your view on how CAESAR8 will be able to assist projects:				
3.1.	Ensuring all stakeholders maintain active involvement in projects				
	4	3	3	4	5
3.2.	Supporting collaboration across separate teams				
	4	3	4	4	4
3.3.	Maintaining an holistic perspective when agreeing changes				
	4	4	4	4	5
3.4.	Obtaining senior management acceptance of project issues and risks				
	4	4	3	4	4
3.5.	Completing legal compliance reviews for all changes				
	4	4	4	4	4
3.6.	Security risk management is understood in a business context				
	4	4	2	4	4
3.7.	Applying rigor when working with third parties				
	4	4	3	4	5
3.8.	Ensuring that agreed security controls are fully implemented				
	4	4	4	4	5
3.9.	Ensuring security controls will be monitored				
	4	4	4	4	4
3.10.	Full understanding of how a new system impacts on current business processes				
	4	4	3	4	5
3.11.	Clarity over information storage and sharing				
	4	4	3	4	3
3.12.	Ensuring that new technology is implemented in a controlled manner				
	4	3	4	4	3
3.13.	Understanding how a new system impacts all effected personnel				
	4	4	4	4	4
3.14.	Ensuring that testing has completed adequately				
	4	3	3	4	4
3.15.	Ensuring that management will monitor system performance				
	4	3	3	4	4
4.	Please rate these other potential CAESAR8 characteristics:				
4.1.	The 40 questions covered some key issues to determine success				
	4	4	4	5	4
4.2.	The 40 questions were easy to understand				
	4	4	3	5	4

4.3.	It was easy to conduct assessments	4	4	4	4	4
4.4.	Conducting assessments was a quick process	4	4	4	4	4
4.5.	It was valuable to include multiple stakeholders when conducting assessments	4	4	5	4	5
4.6.	The levels (1-5) were meaningful	4	4	3	4	5
4.7.	It was easy to share results with all colleagues and management	4	4	4	4	4
4.8.	It was easy to integrate CAESAR8 with existing DevOps and Project processes	4	3	3	3	4
4.9.	CAESAR8 supports integration with Agile working practices	4	3	4	3	4
4.10.	CAESAR8 assists with the prioritization of work	4	3	4	3	4
4.11.	CAESAR8 will help to maintain essential architecture documentation	4	4	4	3	4
5.	Please rate the involvement of other stakeholders:					
5.1.	Additional stakeholders could be from other, non-security roles	4	4	4	4	4
5.2.	The CAESAR8 assessments provided relevant questions for other stakeholders	4	4	3	3	4
5.3.	The stakeholders could identify performance markers that were relevant to them	4	4	2	3	4
5.4.	Stakeholders can provide just the responses where they have knowledge/responsibility	4	4	3	4	4
5.5.	It was easy to combine separate assessments and collaborate on the results	3	4	3	3	4

Table D.9: Post-evaluation 2

Appendix E

Performance Marker Matrix - Question Set

Table E.1 shows the first draft of the CAESAR8 matrix. I have included this early draft because it shows how the themes for the columns and cells were emerging from the literature. The final version of the CAESAR8 matrix has already been provided in Figure 5.10 and shows how each cell was developed into a performance marker question that business stakeholders can answer from their own perspective. When assessed together, these performance markers create the **CAESAR8 checklist**.

This version of the matrix uses the EA domain to provide a definition of the levels.

The full matrix for the first version, the evaluation version and the last version of the performance markers that were used in CAESAR8 prototypes are shown on the following pages.

	Business	Business Change	Security Impact	Security Strategy	Optimization
	1	2	3	4	5
EF	Law and regulations	Budgets for change	Change in external threats	Budgets and contracts	Threat intel optimized
SG	Alignment of risk tools and timescales	Security risks of changes	Security control changes	Residual risks and resources in place	Explicit trust in transformations
BP	Affected business processes	Process changes	Risks of process changes	Controls implemented	Standardized (digitized)
IA	Information and classification	Information changes	Risks of information changes	Controls implemented	Data integration underway
TI	The networks and systems	Changes to technology	Technical impact	Controls tested /assured	Modularization of systems
HF	ALL essential personnel	Changes to personnel	User impact analysis	Personnel trained	Automation
MI	Information Owner engaged	Managers to monitor compliance	Monitoring confirmed	Means to monitor and respond	Good security culture evident
EA	Affected business areas	Effect of business changes	Change impact	Security controls	Supporting EA updated

Table E.1: First version of the CAESAR8 performance marker matrix

CAESAR8	Assessment Stages				
	1	2	3	4	5
Description	Business <i>Corporate/Unit Wholeness</i> All stakeholders* for the relevant service or department must agree performance at each level of this CAESAR8 assessment for the change	Business Change <i>Project Changes</i>	Security Impact <i>Related Security</i>	Security Strategy <i>Changes to Security</i>	Optimization <i>Retrospection for Agility</i>
Enterprise Architecture	Agreement reached on what parts of the business are impacted by project/iteration	All current changes have been considered holistically by stakeholders	Security controls have been identified for this iteration/deployment	Security control changes support the project and the wider enterprise	CAESAR8 elements update enterprise architecture and maturity models
External Factors	All applicable legislation and regulations, have been reviewed and referenced	Budgets have been allocated to meet the potential cost of changes to security controls	Changes to external threats have been assessed	Budgets are sufficient. Security requirements included in third-party contracts	Threat intelligence optimized
Security Governance	Security risk management methods aligned to business risk and risk appetite. All timescales considered	Current business risks of the change are assessed and communicated to all stakeholders	All changes to risk assessments have been concluded and changes to controls highlighted	Residual security risks of changes are accepted, and security resources have been allocated	Explicit trust achieved for business transformations
Business Process	All business process(es) that are affected by the iteration identified and criticality assessment undertaken	Changes to the processing of information, including storage and sharing is provisionally approved	The security risks of the changes to business process(es) have been determined	Security requirements for process changes, including the use of external entities, are established	Standardized and harmonized processes. Digitized static processes
Information Assets	All information that supports the processes is mapped to systems, and classification requirements are reviewed	Corresponding changes that are required to support information processing and storage have been identified	Changes to the security risks of information subject to the changes have been determined	The requirements for protecting all information after this change have been agreed	Data integration initiatives are underway
Technology Infrastructure	Existing networks and information systems that are, or could be, affected by this change are identified	Changes to technology have been identified, including the use of any external services	New/changed technical security controls have been identified to support the change	New/changed technical security controls have been tested and received appropriate assurance	Modularization of systems is being achieved
Human Factors	All personnel groups that are essential to operating the process(es) (internal and external) are identified	Changes to personnel involved in delivering or supporting the process(es) have been identified	User impact analysis has been conducted for new process(es) and technology changes	Personnel have been trained in changes to SOPs and SyOPs, and the use of any new technology	Automation of processes to reduce human error
Management Influence	The Corporate Entity Owner (e.g., head of unit) for the associated information and processes is engaged	Entity (middle) Managers (internal and external) who will monitor security compliance are engaged	New requirements for security monitoring of controls and compliance have been confirmed	Management given the means to monitor all security controls and respond appropriately	Good security culture evident

Figure E.1: Performance Marker Matrix (or Question Set) v1

CAESAR8 Matrix v1.0c	The Business Level 1	Business Change Level 2	Security Impact Level 3	Security Strategy Level 4	Optimization Level 5
EF: External Factors	Stakeholder is compliant with relevant legal, regulatory and corporate requirements	Stakeholder has considered their use of a third-party organization	Resultant changes to stakeholder's security threats have been assessed	Stakeholder's budgets are adequate to meet security control changes	Stakeholder believes threat intelligence is optimized in relation to this change
SG: Security Governance	Stakeholder has reviewed all security risks related to the business area under change	Stakeholder's critical objectives for the change, incl. timescales, have been shared	Security and stakeholder risk management methods are aligned, e.g., risk appetite	Security controls and residual risks are agreed with stakeholder	Stakeholder confirms change removes any implicit trust and adheres to least privilege concepts
BP: Business Process	Stakeholder has assessed the criticality of all business processes affected by this change	Stakeholder has clarified all resulting changes to information processing, including sharing	Risks of the changes to stakeholder's business process(es) have been determined	Stakeholder has agreed new security measures for process changes, incl. 3rd party contracts	Stakeholder confirms standardized and harmonized processes. Static processes digitized
IA: Information Assets	Stakeholder is aware of their information that is affected, and this is mapped to systems	Stakeholder has reviewed any requirement to move data out of core systems	Changes in stakeholder security risks for data transmission, retention and storage are shared	Stakeholder has agreed all requirements for protecting information post change	Data integration initiatives are underway from stakeholder perspective
TI: Technology Infrastructure	Stakeholder is aware of all networks and systems potentially affected by this change	Changes to technology are confirmed with stakeholder, incl. use of any external services	All required changes to technical architecture have been confirmed with stakeholder	Stakeholder is aware of a documented plan to test the changes to technology	Stakeholder confirms modularization (loose coupling) of systems to increase flexibility
HF: Human Factors	Stakeholder identified all personnel operating the current process(es) (internal and external)	Stakeholder has identified their personnel that deliver or support the change	Stakeholder reviewed results of user impact analysis for process and technology changes	Stakeholder agrees program for recruiting and training all applicable resources	Stakeholder confirms automation of processes to reduce human error
MI: Management Influence	Stakeholder is aware of the active involvement of the owner(s) of the data and processes	Stakeholder has appointed responsibility for monitoring security compliance	Stakeholder accepts documented requirement to monitor security compliance	Stakeholder has the means to monitor all security controls and respond appropriately	Good security culture evident for stakeholder
EA: Enterprise Architecture	A reference architecture covers related business segments from stakeholder perspective	Draft artifacts describe the transitional target architecture for stakeholder's changes	A full security impact assessment covers transition from stakeholder perspective	The security strategy includes all architecture changes required by stakeholder	Documentation for the reference architecture includes stakeholder

Figure E.2: Performance Marker Matrix (or Question Set) v1c

V 2 (b&w)	The Business Level 1	Business Change Level 2	Security Impact Level 3	Security Strategy Level 4	Optimization Level 5
EF: External Factors	Stakeholder is compliant with relevant legal, regulatory and corporate requirements	Stakeholder is aware of their dependence on third-party organizations	Stakeholder has checked for any consequential changes to security threats	Stakeholder's budgets are adequate to meet security control changes	Stakeholder believes threat intelligence is optimized in relation to this change
SG: Security Governance	Stakeholder has reviewed all security risks related to the business area under change	Stakeholder's critical objectives for the change, incl. timescales, have been shared	Security and stakeholder risk management methods are aligned, e.g., risk appetite	Security controls and residual risks are agreed with stakeholder	Stakeholder confirms change removes any implicit trust and adheres to least privilege concepts
BP: Business Process	Stakeholder has assessed the criticality of their business processes that are affected by this change	Stakeholder has clarified all resulting changes to information processing, including sharing	Risks of the changes to stakeholder's business process(es) have been determined	Stakeholder has agreed new security measures for process changes, incl. 3rd party contracts	Stakeholder confirms standardized and harmonized processes. Static processes digitized
IA: Information Assets	Stakeholder is aware of their information that is affected, and this is mapped to systems	Stakeholder has reviewed any requirement to move data out of core systems	Changes in stakeholder security risks for data transmission, retention and storage are shared	Stakeholder has agreed all requirements for protecting their information post change	Data integration initiatives are underway from stakeholder perspective
TI: Technology Infrastructure	Stakeholder is aware of all networks and systems potentially affected by this change	Changes to technology are confirmed with stakeholder, incl. use of any external services	All required changes to technical architecture have been confirmed with stakeholder	Stakeholder confirms that testing is documented and executed satisfactorily	Stakeholder confirms modularization (loose coupling) of systems to increase flexibility
HF: Human Factors	Stakeholder identified all personnel operating the current process(es) (internal and external)	Stakeholder has identified their personnel that deliver or support the change	Stakeholder has reviewed the results of user impact analysis for all changes	Stakeholder agrees program for recruiting and training all applicable resources	Stakeholder confirms automation of processes to reduce human error
MI: Management Influence	Stakeholder is aware of the active involvement of the owner(s) of the data and processes	Stakeholder has appointed responsibility for monitoring security compliance	Stakeholder accepts documented requirement to monitor security compliance	Stakeholder has the means to monitor all security controls and respond appropriately	Good security culture evident for stakeholder
EA: Enterprise Architecture	A reference architecture covers related business segments from stakeholder perspective	Draft artifacts describe the transitional target architecture for stakeholder's changes	A full security impact assessment covers transition from stakeholder perspective	The security strategy includes all architecture changes required by stakeholder	Documentation for the reference architecture includes stakeholder

Figure E.3: Black and White performance marker matrix (or Question Set) v2

Appendix F

Web app screenshots

This web app instantiation of CAESAR8 was created for the purposes of the evaluation only. To help volunteer experts to gain essential knowledge about the evaluation and prepare as quickly as possible, all instructions, videos and defaults were presented immediately in this single instruction page. The key areas were indicated with MUST WATCH and MUST READ.

The volunteers were then provided with a page to capture their assessments and another page to combine the assessments and view the results.

The following screenshots are included in this chapter:

Screenshot	web app Area	Additional Information
1	CAESAR8 Homepage	Volunteer experts were presented with a default home page initially. This page included a tutorial video and all evaluation instructions.
2	Assessment Page	All assessments conducted in the web app were carried out in the assessments page, which included a few navigation options to assist volunteers. It can be seen how the generic term “stakeholder” was replaced with actual name given for the stakeholder completing the assessment.
3	Results Page	Once assessments had been completed, the results could then be viewed in the CAESAR8 radial model. The assessments could be combined in any combination, so that the effect could be examined closely.
4	Tutorial videos	All volunteers were provided with a 10 minute tutorial to ensure that they all had the same training. A short 3 minute video was also provided to explain the model itself.
5	Default options	The instructions included an area where defaults could be captured there and then, to assist volunteers in completing the evaluation.

Table F.1: CAESAR8 web app Screenshots

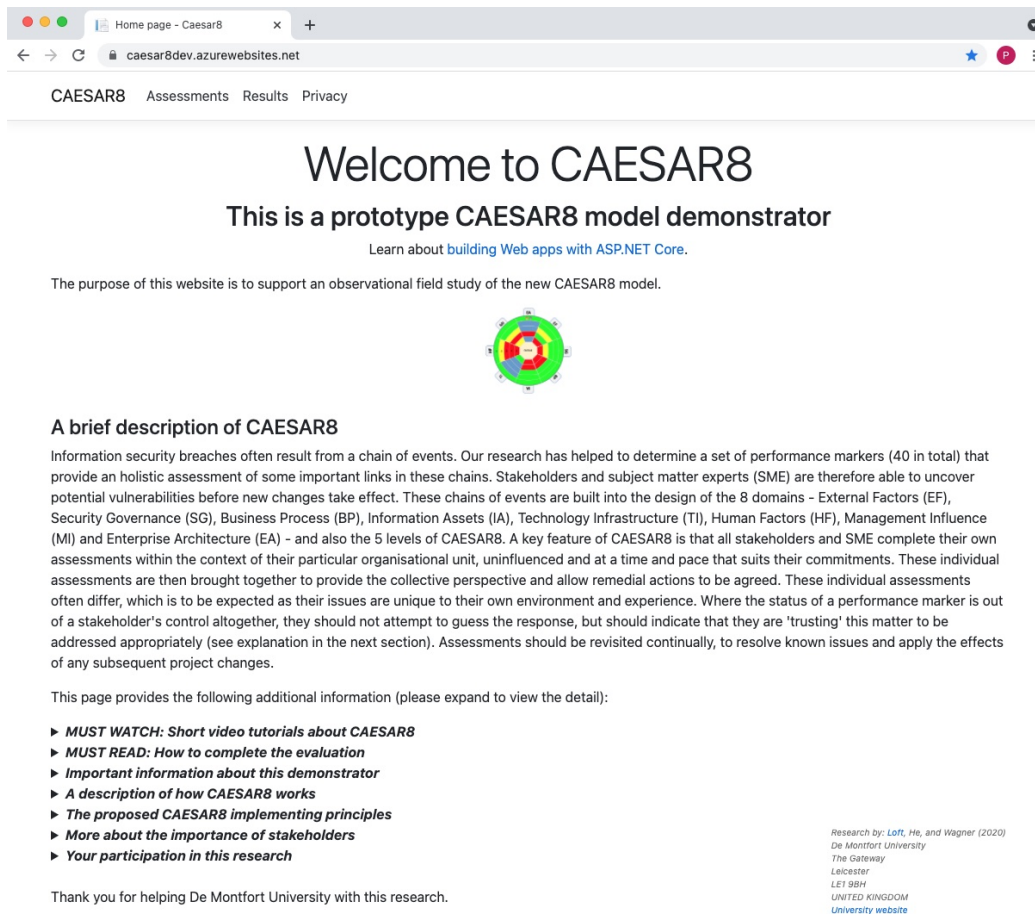


Figure F.1: The web app Home Page

CAESAR8 Assessment - Caesr x +

caesar8dev.azurewebsites.net/Assessment?__RequestVerificationToken=CfDJ8N-EIS2p8tVAgzAssOeERD144Dmdh93xJ7T4ndzdHshQK9AYtjG... ☆ P

CAESAR8 Assessments Results Privacy

CAESAR8 Assessment

Scope

Please select a valid project and stakeholder. You can also enter a new project and/or stakeholder to create a new assessment

User ID: 4LOq Project: Simulation Stakeholder: Researcher 2 Clear Project Edit Assessment

Assessments found: Researcher 1, Researcher 2 (2 assessments)

Edit Previous 4LOqSimulationResearcher 2

Assessment Form

Please complete assessment below and click 'Finish Assessment' when done (changes are saved automatically as you progress) Finish Assessment

- Yes (green on model) – from the assessor’s perspective, this issue is relevant and has been met
- No (red on model) – whilst relevant, this requirement has not been met
- Partial (yellow on model) – the assessor wishes to indicate that work in this area has started but is not complete
- Trust (blue on model) – relevant for stakeholder, but trusting another party to action. Examine evidence before changing final assessment
- Not applicable (black on model) – the question is deemed 'Not Applicable' for assessor
- (unknown) (grey on model) – no answer is currently given

Researcher 2's assessment for Simulation

Level 1 Questions		
EF1	Researcher 2 is compliant with relevant legal, regulatory and corporate requirements	Yes include any notes
SG1	Researcher 2 has reviewed all security risks related to the business area under change	Yes include any notes
BP1	Researcher 2 has assessed the criticality of all business processes affected by this change	Yes include any notes
IA1	Researcher 2 is aware of their information that is effected, and this is mapped to systems	Yes include any notes
TI1	Researcher 2 is aware of all networks and systems potentially affected by this change	Yes include any notes
HF1	Researcher 2 has identified all personnel operating the current process(es) (internal and external)	Yes include any notes
MI1	Researcher 2 is aware of the active involvement of the owner(s) of the data and processes	Yes include any notes
EA1	A reference architecture covers related business segments from Researcher 2 perspective	Yes include any notes
Level 2 Questions		
EF2	Researcher 2 is aware of their dependence on third-party organisations	Yes include any notes
SG2	Researcher 2's critical objectives for the change, incl. timescales, have been shared	Yes include any notes
BP2	Researcher 2 has clarified all resulting changes to information processing, incl. sharing	Yes include any notes
IA2	Researcher 2 has reviewed any requirement to move data out of core system(s)	Yes include any notes
TI2	Changes to technology are confirmed with Researcher 2, incl. use of any external services	Yes include any notes
HF2	Researcher 2 has identified their personnel that deliver or support the change	Yes include any notes
MI2	Researcher 2 has appointed responsibility for monitoring security compliance	No Only Complaints, not for Purchasing
EA2	Draft artifacts describe the transitional target architecture for Researcher 2's changes	No Not completed
Level 3 Questions		
EF3	Resultant changes to Researcher 2's security threats have been assessed	Yes include any notes

Figure F.2: The Assessment page of the web app

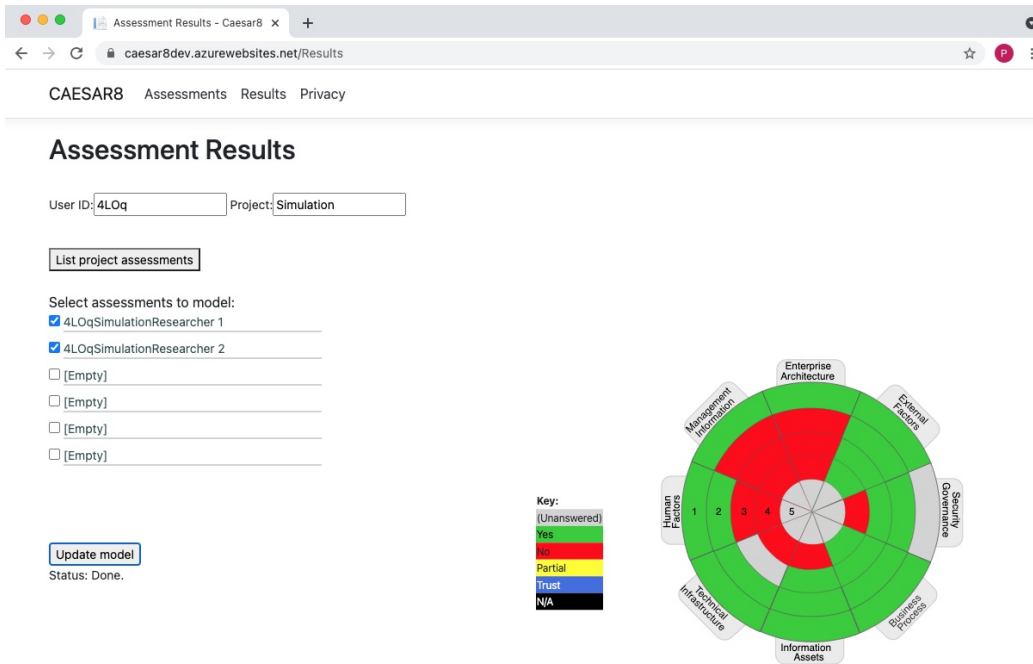



Figure F.3: The Results page of the web app

Home page - Caesar8
caesar8dev.azurewebsites.net

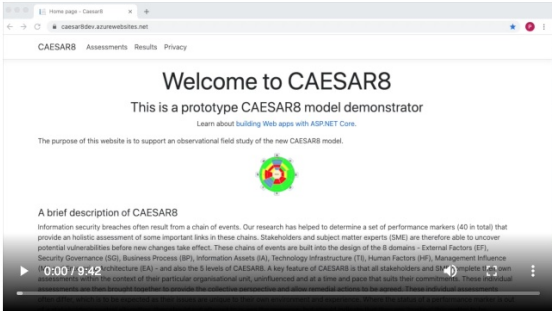
▼ MUST WATCH: Short video tutorials about CAESAR8

The purpose of these videos is to give you all the information that you'll need to conduct the evaluation of CAESAR8. There are two videos: a 3-minute thesis to describe the science behind the new CAESAR8 model, and a second video to describe how to use this app. It is important to mention that this field study is not an evaluation of the App. We have created the App to make it easier to test the model. The evaluation is of the CAESAR8 model itself.

A 3 minute video to explain the science behind the new CAESAR8 model:



A 10 minute video to explain how to use the CAESAR8 evaluation web app:



► MUST READ: How to complete the evaluation

► Important information about this demonstrator

► A description of how CAESAR8 works

► The proposed CAESAR8 implementing principles

► More about the importance of stakeholders

Research by: Loft, He, and Wagner (2020)
De Montfort University

Figure F.4: Training videos featured in the web app

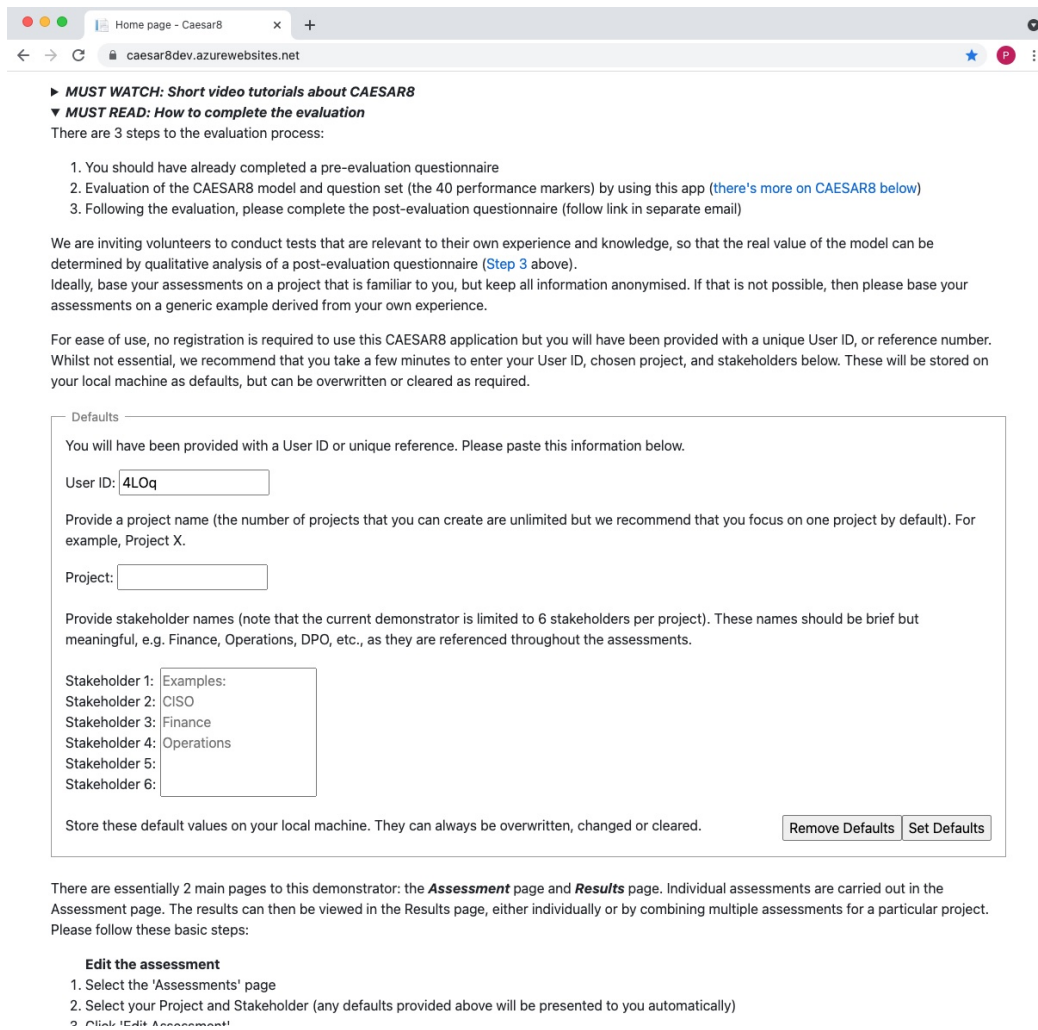


Figure F.5: Default options captured in the web app

Appendix G

Case study - synthetic scenario

The scenario is described as follows:

Company X's Design and Marketing Departments have made the decision to outsource the delivery of one of its services to a third party, known as Company Y. Company X has been delivering this service itself for almost 10 years. Whilst not critical to their success, it is still a valuable service, as it draws in crucial customers. However, it is very specialist and the costs for delivering this service in-house are becoming prohibitive.

Agreement has been reached with Company Y on charges, and these are even cheaper for the consumer, whilst still being profitable for both companies.

Company X will maintain exclusive rights to sell this service via its own website.

Company X's CEO and Purchasing Manager have discussed these issues and have agreed to collect orders for this service as normal but will then send applicable part-orders digitally to Company Y. They expect this to be approx-

imately 5000 orders per year.

Company X has identified the changes that are required to its Purchase Order computer system, which will transmit orders to Company Y's computer system, via a new TLS encrypted Internet data link. Minimal information for fulfilling client orders will be transferred, and this will contain limited personal information, such as name and address. No billing data to be sent. These changes have been fully costed. The Board has agreed with the Purchasing Manager that it will meet the costs of making the changes to the Purchasing System and would like to know details of any additional costs. Company Y will invoice Company X for all delivered services on a monthly basis.

The supervisor for the purchasing team has been made aware of the change and considers that there will be no impact on the purchase process, as this is an online ordering service only.

The Board have confirmed that Company X will still process all client complaints and will consult with Company Y as required for their services. The CEO of Company X has spoken to Company X Complaints Manager about the proposals. The Complaints Manager has explained how Company X Complaints Department uses a separate CRM system and will therefore share relevant complaint information with Company Y. The Complaints Manager has advised that they have very few complaints for this service and can manage these on an ad-hoc basis without any additional cost.

The CRM system has the same data classification as the Purchase Order system, although it is less critical in terms of availability.

Company X has identified that no other parts of the business are affected by

this change.

Some of Company X's design staff have elected to take redundancy or take different jobs at Company X, but many will be transferred to Company Y, under TUPE arrangements, and will deliver this service as normal. Company Y already has some staff who are trained in this service.

Company Y will use Company X branding on all related services.

Company X will continue to guarantee this service for 2 years.

A future date has been set for when this service will be transferred to Company Y and all agree that this is achievable.

Company X's Risk Manager has been reviewing the changes to the Purchasing System with a number of Company X's SMEs, including the Legal Advisor, Data Protection Officer, IT Manager and the CISO. They have been assessing the risks and mitigations in relation to information management and security. The Purchasing Manager has also been engaged in these discussions to ensure risk assessments are aligned with the business needs.

Company X Legal Department has helped SMEs to review all applicable legislation and regulations and is now drafting a contract with Company Y for how purchasing data is to be protected and retained, as they will be a data processor.

The CISO has revised the threat assessment for Company X and has identified an increased risk of attack from the new connection with Company Y. Company Y has already achieved an ISO/IEC 27001 certification for a part of its network services and offers this existing assurance to Company X.

Company X and Company Y have agreed to complete a full test of external facing systems and connections before the changes go into production.

A basic schema for the case study scenario is shown in Figure G.1

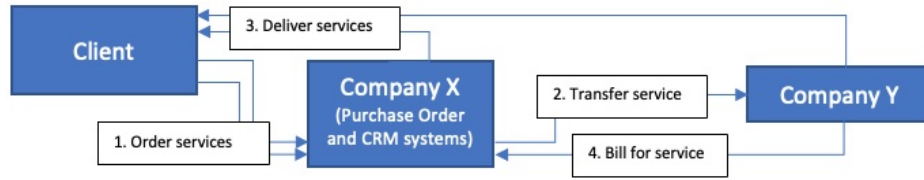


Figure G.1: Basic schema for the synthetic scenario

Appendix H

Explaining the origins of the artifact to volunteers

The following transcript was provided to volunteer experts involved in the evaluation of CAESAR8:

- CAESAR8 is not a new security maturity framework, or a new security standard or risk methodology. It is an entirely new model that recognizes the significance of following enterprise architectural principles when implementing information security solutions – of which the benefits have been proven by scientific studies.
- However, CAESAR8 benefits from new analysis of the common causes of failures for information security, even where a good security posture exists for the organization.
- At the heart of the model is a 8 x 5 matrix. The rows form the 8 domains which have been derived from scientific studies of past failures. These are arranged in 5 levels which provide an ordered sequence for identifying the environment that is affected by the proposed change, through to analyzing the security impact,

together with supporting strategies and opportunities for optimization.

- This matrix provides 40 different tests, which we call Performance Markers. These performance markers could be regarded as a standard checklist, and are based on a study of most significant correlations across the 8 domains. They are, therefore, key when establishing whether projects are considering the most influential factors that ultimately determine success or failure.
- The results are then shown in a radial model that is easy to share at all levels of the organization.
- An important factor in these reviews is that they must be conducted independently by all key stakeholders. These individual assessments are then brought together using a standard set of rules, which will provide the overall status of enterprise security for the change project.
- Stakeholders and SMEs should make use of recognized standards, where appropriate, but they must also use their own knowledge and experience when determining whether their requirements have been met.
- By focusing on these key factors, CAESAR8 helps to prevent some critical omissions and oversights that can prove so damaging for new projects. This also makes the model suitable for Agile business change projects, where quick and continuous reviews are important. Enterprise Architecture and agile are sometimes seen as contradictory concepts, but CAESAR8 helps to bring these disciplines together, and encourages ‘just-enough’ architecture documentation.
- All Performance Markers should be reviewed continuously to ensure that all project changes are reviewed and that controls remain effective. By combining multiple security assessments at just the right level, CAESAR8 supports the integration of Information and Operational Technology (or IT and OT) and even safety assessments into a single assessment for a given solution.