UNIVERSITÉ DE SHERBROOKE
École de gestion

Conception d'un tableau de bord stratégique en sécurité de l'information pour le soutien de la conscience de la situation

Par
Nicolas Blain

Mémoire présenté à l'école de gestion
En vue de l'obtention du grade de
Maîtrise ès sciences, M. Sc.
Stratégie de l'intelligence d'affaires

Janvier 2021

UNIVERSITÉ DE SHERBROOKE
École de gestion

Conception d'un tableau de bord stratégique en sécurité de l'information pour le soutien de la conscience de la situation

Nicolas Blain

A été évalué par un jury composé des personnes suivantes :

_____ Membre du jury
(Daniel Chamberland-Tremblay)

_____ Membre du jury
(Marc Frappier)

_____ Codirecteur de recherche
(Alexandre Moïse)

_____ Codirecteur de recherche
(Pierre-Martin Tardif)

Mémoire accepté le _____

SOMMAIRE

Le responsable de la sécurité des systèmes d'information (CISO) a pour objectif de s'assurer que le conseil d'administration et les hauts dirigeants ont une bonne compréhension de la situation actuelle de l'organisation en matière de sécurité de l'information, puis d'agir de conseiller stratégique pour les décisions qui ont un impact sur la sécurité de l'information. Pour atteindre ces objectifs, le CISO doit avoir accès à de l'information fiable et complète, au moment opportun. Comme la reddition stratégique d'une telle quantité d'information est un processus complexe, elle nécessite l'utilisation d'outils comme le tableau de bord de gestion, défini comme étant un résumé en une page de l'information critique qui permet à l'utilisateur d'atteindre ses objectifs. Cet article propose une méthode de conception de tableau de bord stratégique en sécurité de l'information pour le soutien de la conscience de la situation, qui permet à une partie prenante stratégique en sécurité de l'information d'avoir une bonne compréhension de son environnement. Ensuite, l'article offre un aperçu de la valeur de cette méthode en présentant une maquette de tableau de bord, conçue pour le CISO d'une institution financière canadienne et son équipe. Il documente aussi les défis rencontrés lors du processus de conception.

RÉSUMÉ

Les technologies de l'information deviennent rapidement indispensables à la mission de nombreuses organisations. Ce changement de paradigme s'accompagne d'une nouvelle réalité pour la sécurité de l'information. Si celle-ci est une contrainte dans les décisions liées aux technologies de l'information depuis longtemps, il est beaucoup plus récent qu'elle ait aussi une importance de premier plan dans les décisions stratégiques des organisations. C'est dans ce contexte qu'émerge le rôle de responsable de la sécurité des systèmes d'information (CISO), responsable de la gouvernance et de la gestion de la sécurité de l'information. La gouvernance en sécurité de l'information est définie au sens large comme le rôle qui assure que les besoins stratégiques de l'entreprise sont clairement définis et que le programme de sécurité remplit ces besoins. La gestion de la sécurité de l'information, quant à elle, vise à planifier et à exécuter les activités qui permettent d'atteindre ces buts (ISACA, 2012). Pour atteindre ces objectifs stratégiques de la sécurité de l'information, il est crucial pour le CISO d'avoir accès à la bonne information, au bon moment. Un outil, largement utilisé en gestion dans le processus de reddition est le tableau de bord de gestion. Défini comme « une représentation visuelle de l'information critique qui est requise pour arriver à un ou plusieurs objectifs, consolidé en un seul écran pour que toute l'information soit accessible simultanément », le tableau de bord de gestion permet essentiellement d'afficher des indicateurs de manière à « procurer une conscience de la situation véridique et complète à son utilisateur » (Few, 2013). La conscience de la situation (CS) est définie comme étant la perception des éléments de l'environnement dans un volume de temps et d'espace (niveau 1), la compréhension de leur signification (niveau 2) et la projection de leur état dans un futur proche (niveau 3).

Bien que l'idée d'appliquer la CS à la sécurité de l'information ait été explorée auparavant (Franke & Brynielsson, 2014), conduisant même à certaines applications au niveau stratégique (Webb et al., 2014), elle a rarement été utilisée dans la conception de tableaux de bord de sécurité de l'information, en particulier au niveau stratégique. Si nous acceptons l'idée proposée par Few (2013) selon laquelle les tableaux de bord améliorent la qualité des décisions en améliorant la CS de l'utilisateur, alors il semble logique de combiner

les apprentissages qui viennent de la recherche sur la CS aux démarches existantes de conception de tableaux de bord de gestion. Cela nous amène à la question de recherche explorée dans ce projet de recherche : comment concevoir des tableaux de bord stratégiques de sécurité de l'information pour le soutien de la CS? Pour répondre à cette question, la méthode de conception pour soutenir la CS (Endsley & Jones, 2011), est adaptée à un contexte stratégique en sécurité de l'information. Cette adaptation s'inscrit dans une démarche de recherche en science de la conception, une méthode qui vise à résoudre des problèmes organisationnels de façon innovatrice à travers la création d'artéfacts (Hevner et al., 2004). La recherche en science de la conception rend possible de concevoir quatre formes d'artéfact : un construit, un modèle, une méthode et une instance (March & Smith, 1995). Dans notre cas, une méthode de conception de tableau de bord est proposée, puis appliquée pour concevoir une instance en collaboration avec une institution financière canadienne.

La méthode proposée dans l'article se déroule en 3 phases, à l'instar de la méthode proposée par Endsley & Jones (2011). La phase 1 consiste à déterminer les besoins de manière à soutenir la CS de l'utilisateur en identifiant l'information à laquelle un utilisateur aurait accès dans un monde idéal, à travers la démarche d'analyse des tâches dirigées par les buts. Ce processus est conduit à travers une série d'entrevues, dans notre cas avec sept parties prenantes stratégiques de l'institution financière, et mène à la création d'une hiérarchie de buts, de décisions et d'exigences CS qui seront affichées dans le tableau de bord de gestion. La phase 2, guidée par huit principes fondamentaux de conception pour le soutien de la CS et par les bonnes pratiques de conception de tableau de bord de gestion proposées par Few (2013), se déroule sous la forme d'un processus itératif qui mène à la maquette de tableau de bord de gestion. L'article présente l'évolution de cette maquette et les défis rencontrés lors de la conception de celle-ci. La phase 3 vise à s'assurer de l'atteinte réelle de la CS par l'utilisateur avec une méthode d'évaluation robuste. Dans notre cas, cette démarche d'évaluation a été réalisée pour plusieurs versions de maquette, avec au total six parties prenantes de l'institution financière. Pour ce faire, elle s'inspire fortement de la technique d'évaluation globale de la CS proposée par Endsley & Jones (2011), mais est adaptée pour être plus facile concevoir, à exécuter et à mettre à jour.

Après avoir mis en lumière les limites des méthodes existantes de conception de tableaux de bord stratégiques en sécurité de l'information, ce projet de recherche crée de la valeur pour les experts en sécurité de l'information en proposant une méthode qui permet de créer de meilleurs tableaux de bord de gestion. De plus, elle décrit les problèmes rencontrés en cours de conception ainsi que les solutions qui nous ont permis de régler ces problèmes.

L'article proposé a été écrit par Nicolas Blain, Alexandre Moïse, Pierre-Martin Tardif et Annie-Claude Pellerin. Il sera soumis pour publications à la revue Computers and Security.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

DESIGNING A STRATEGIC INFORMATION SECURITY DASHBOARD TO SUPPORT SITUATION AWARENESS

Abstract

The Chief Information Security Officer (CISO) is the senior-level executive who ensures that the board and the executives have a good understanding of the current information security posture of the organization. To fulfill this objective, the CISO needs to have access to reliable, complete and relevant information in a timely manner to allow them to communicate effectively and to take the best decisions. Widely viewed as a great enabler of good performance management, the dashboard is a one-pager summary of the information that allows users to meet their objectives. This paper describes a method that makes it possible to consistently design dashboards that support situation awareness, giving users a good understanding of their environment in order for them to reach their goals. It then creates an example of such a dashboard that targets information security strategic stakeholders such as the CISO in the context of a Canadian financial institution, giving insights into the challenges faced in the design process.

1. Introduction

Information security has been increasingly important for organizations, going from a concern mostly addressed by IT departments a few years ago to become a regular topic of discussion at the board-level. To account for this heightened importance, the role of the Chief Information Security Officer (CISO) emerged. The CISO is the most senior role in the corporate hierarchy to have information security as its core responsibility, ensuring that organizational information security objectives are clearly defined and aligned with the overarching business objectives. Once those objectives are agreed upon, the CISO is also responsible for the planning and the execution of the activities that compose them (ISACA, 2012). To successfully achieve the goals of strategic information security, the CISO must derive insights from a large quantity of information. We argue that the dashboard is one of the best tools to communicate such information, leading to better decisions, which in turn improve the information security posture of the organization.

A dashboard is defined as "a visual display of the most important information needed to achieve one or more objectives that has been consolidated on a single computer screen so it can be monitored at a glance." (Few, 2013). In order to be effective, a dashboard needs to display performance and risk indicators in a way that provides the user with a complete and accurate situation awareness (Few, 2013). This concept of situation awareness (SA) describes the mechanisms through which individuals understand what is happening in their environment. A complete and accurate SA means the user has extracted and properly processed all the required information from the environment, allowing them to make decisions on the adequate course of action to achieve specific goals.

1.1. Research problem and research question

While the idea of applying SA to information security has been explored to quite some length (Franke & Brynielsson, 2014), even leading to some applications at the strategic level (Webb et al., 2014), it has seldom been used in information security dashboard design, especially at the strategic level, as highlighted by the literature review presented in section 3. If we accept the idea proposed by Few (2013) that dashboards improve the quality of decisions by improving the user's SA, then applying what has been learned in SA research to strategic information security dashboards seems to be a great path to better dashboards. That leads us to the research question explored in the current research paper: How to design information security strategic dashboards that support SA?

1.2. Paper outline

In order to give insight into this question, the paper is organized in four sections. First, section 2 defines the underlying concepts of SA and SA-oriented Design (SAOD). Then, section 3 presents a systematic review of the existing literature on information security dashboards and an assessment of their ability to support their user's SA. Section 4 subsequently presents the selected research methodology, Design Science Research. The result of this research process is a method to design information security strategic dashboards based on SA-oriented Design. This method has then been instantiated, leading to a mock-up for a strategic information security dashboard, designed with of a Canadian financial institution. These two artifacts, the method and the instantiation, are then detailed in the results in section 5, and their significance is discussed.

2. Situation Awareness

2.1. Definition of SA

SA is defined as the perception of the elements that compose the environment in a volume of time and space (level 1), the understanding of their meaning in relation to a specific goal (level 2) and the anticipation of their evolution in the short term (level 3) (Endsley, 1995b). Explained simply, individuals with a good SA will have a robust understanding of what is happening around them.

Figure 1 presents the theoretical SA model, where SA is the internal representation an individual has of the external environment. Therefore, the robustness of SA has an impact on the quality of the decision taken, which itself affects the external environment when it is turned to an action.

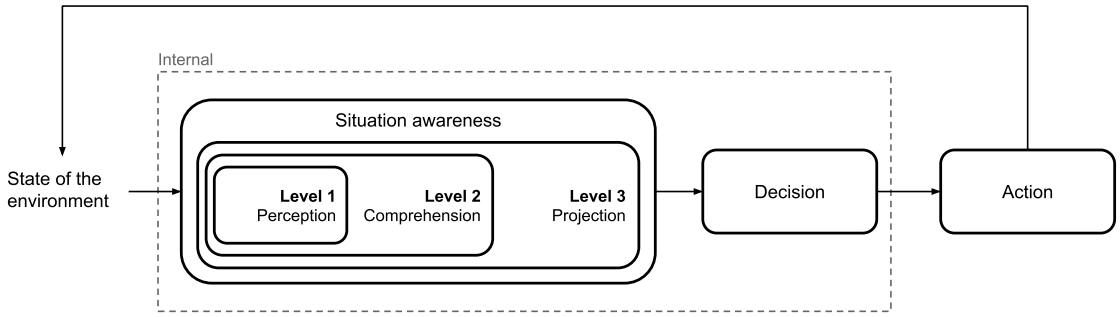

Figure 1. SA Model, adapted from Endsley (1995b)

SA is crucial to the decision. It can be difficult, if not impossible, to make a good decision without an accurate and complete mental representation of the situation. Conversely, a perfect SA could still lead to a poor decision due to external factors such as inadequate expertise, organizational procedures or a troubled state of mind. Thus, even though the decision strongly relies on SA, they are two distinct concepts (Endsley, 1995b).

SA depends on the user's long-term memory to store information as mental models and mental schemas. These mental models are the internal representation made of an external

reality, of the environment in which the user operates. They can be incomplete or imperfect, but ease information processing and allow the user to generate previsions of the future state of the environment. As the user gains experience, mental schemas are also developed. Wherever generalizations can be made from the mental model by identifying prototypical situations, mental schemas will be made to store these rules. That will in turn allow the user to quickly classify a situation as having similar characteristics to a known situation, and to reach a decision faster, with less cognitive effort (Endsley, 1995b).

2.2. Designing for SA

Applying the theory of SA to design problems in the broader framework of user-centered design has led to the approach of SAOD. This design process is built in three phases: (1) a systematic analysis of the requirements, (2) the design of the artifact respecting human-centered SA-oriented design principles, and (3) a reliable evaluation of the actual SA reached by the user (Endsley & Jones, 2011).

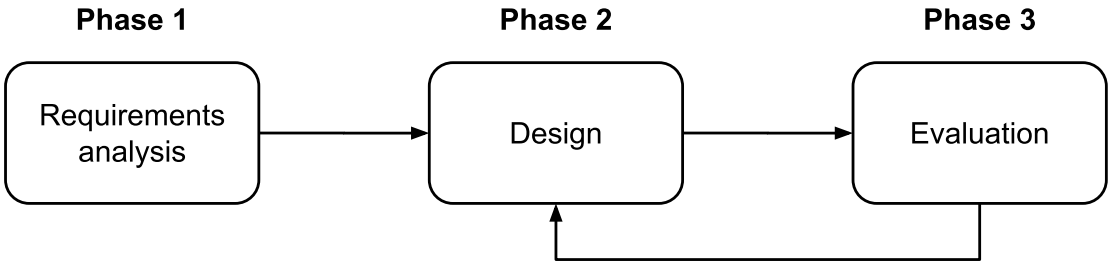

Figure 2. SAOD process, adapted from Endsley & Jones (2011)

2.2.1. Phase 1: Requirements analysis

In order to design an adequate solution, the designer needs a sound understanding of the informational needs of the user and of the context in which the decision occurs. The process of Goal-directed task analysis (GDTA), a form of cognitive analysis, allows the designer to gather this information in a structured way. The GDTA is focused on the goals

of the user, disconnected from the technological constraints that the user faces. It aims to identify the information to which the user would have access in an ideal world, enabling goal driven decision-making (Endsley et al., 2003).

The GDTA process typically relies on interviews with the end users to create a hierarchy of goals and decisions. Figure 3 presents the result of this process, formed of goals, sub-goals, then decisions—which are typically documented with the question that leads to the decision—, and finally the SA elements (informational needs) that enable these decisions in order to maintain the SA of the user.

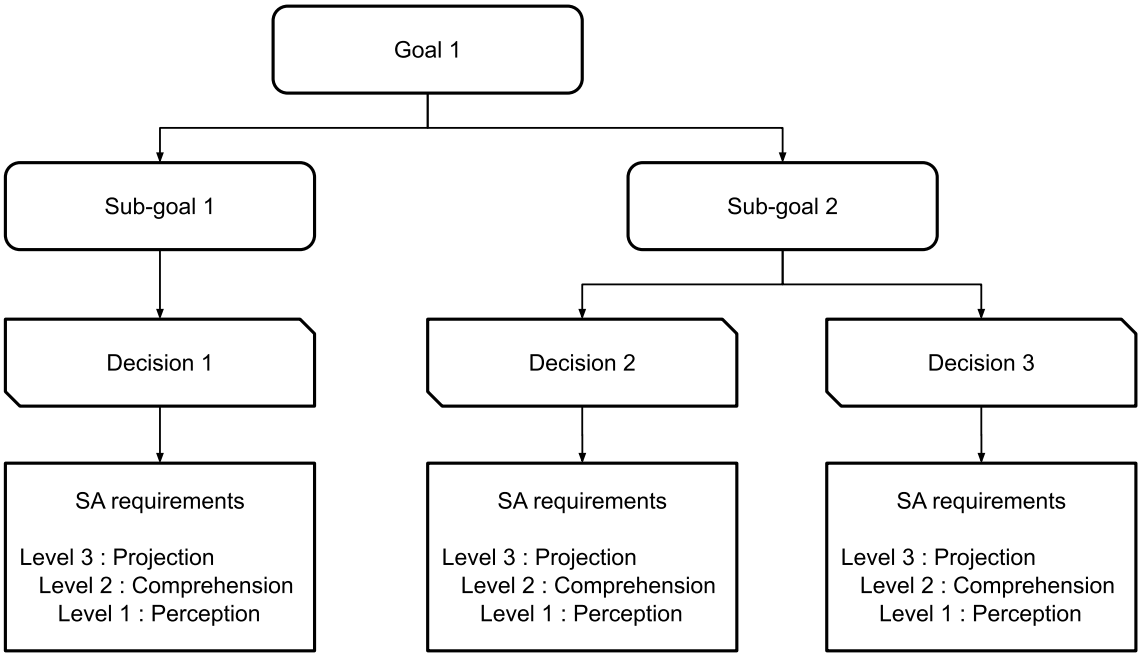

Figure 3. Goal-Decision-SA structure, adapted from Endsley & Jones (2011)

2.2.2. Phase 2: Design

To adequately design a user interface that supports SA, 62 design principles are detailed, divided in 7 categories (Endsley & Jones, 2011). The first category, described as the fundamentals, contains 8 principles. Since they are considered the core foundation of SAOD, they will be the basis of further analysis in section 3.2.

	Principle	Description
1	Organize information around goals	The information displayed needs to be organized around the user's goals, not based on the data source or other technological constraints.
2	Present Level 2 information directly—Support comprehension	The information displayed should have been treated to support the user's comprehension directly. Elements such as the gap between an expected value and a current value should be displayed directly rather than having the user calculate the difference.
3	Provide assistance for Level 3 SA projections	A trend derived from the data should be displayed, if possible, to help the user anticipate the evolution of the situation adequately.
4	Support global SA	The display should offer a high-level overview of the situation to ensure all the elements required to make decisions are available. It shouldn't direct attention of the user to a subset of the information.
5	Support trade-offs between goal-driven and data-driven processing	The interface must promote an efficient shift between the two information processing mechanisms. While principle 1 supports goal-directed information processing, principle 4 promotes adequate prioritization between the goals by supporting data-directed information processing.
6	Make critical cues for schema activation salient	Known signals indicating the link to a prototypical situation should be emphasized to stimulate the activation of the mental model. As an example, a car dashboard presents a light signal indicating low fuel level, triggering the activation of a mental schema to answer the decision: can I reach my destination without stopping to get fuel?
7	Take advantage of parallel processing capabilities	The forms of communication should be varied to harness the user's parallel processing capabilities. The dashboard format limits sensory perception to the visual system. It's still possible to increase the bandwidth of information

	Principle	Description
		processed through the eyes with a good use of the complementary visual channels and varying codes of information processing (Wickens, 2002).
8	Use information filtering carefully	Filters should seldom be used. It could seem well intended to filter information dynamically, restricting it to what's needed to take the current decision and avoid information overload. However, if not applied carefully, this can lead to degrading global SA and reducing the ability of the user to anticipate the evolution of the situation in the short-term.

Table 1. Fundamental design principles summary, adapted from Endsley & Jones (2011)

2.2.3. Phase 3: Evaluation

The evaluation phase allows to determine whether the designed interface provides a complete and accurate SA to its user in a real-world scenario. However, since SA is constructed from the user's mental model, which is internal and hard to make explicit, it's a challenge to evaluate SA directly. The Situation Awareness Global Assessment Technique (SAGAT) is proven to be a viable technique for measuring SA in various contexts (Endsley, 1995a).

The first step of the SAGAT is to create a set of queries that corresponds to all SA elements identified during the SA requirements analysis phase. Then, a simulation is conducted. While the user consults the designed interface, the simulation is put on hold and queries are displayed to the user. For each query, the answer and time required to answer are collected. This technique directly measures the user's SA by assessing the three components of SA: perception, understanding and capability for projection.

While they tend to be objective, direct measuring techniques such as the SAGAT often are intrusive, leading to a degradation of the measured SA by requiring some of the user's cognitive resources to answer the questions. To mitigate this bias, the SAGAT places the simulation on hold before asking questions, a method known as the freeze technique (Endsley, 1988).

3. Systematic Literature Review

In the context of governance and management of information security, tools like the dashboard are widely used to enable effective decision-making and should have been studied thoroughly. While it has been the case outside the strategic level, with over 700 peer-reviewed articles mentioning information security dashboards, almost no research exists at the strategic level. This section, result of a systematic literature review, highlights the key research on (1) information security strategic dashboards, and (2) the use of SA in information security dashboards.

3.1. Research Method

The systematic literature review methodology, initially from the medical field, is now used in multiple disciplines including management (Tranfield et al., 2003). This methodology focuses on comprehensiveness, transparency and reproducibility in order to develop a reliable knowledge base. To that end, the literature review is carried out in three phases: (1) planning the literature review by presenting the objectives and the research questions, (2) conducting the research in a replicable way, leading to a concise state of the existing knowledge on the research questions in a format useful in practice, and (3) reporting the results to make them accessible, sharing this new knowledge.

3.1.1. Planning the review

The literature review plan is presented in table 2. This plan is formalized to ensure repeatability of the process and help protect objectivity by increasing transparency. Considering the lack of publications about dashboards supporting SA in strategic information security, for which no peer-reviewed papers have been found, the subject of the literature review has been established in two parts: (1) information security strategic dashboards, and (2) information security dashboards supporting SA. The concept of dashboard has been

broadly defined to identify all possibly relevant papers, including research terms such as *visualization*, which is often preferred at the operational level in information security, as well as terms such as *scorecard*, *reporting*, or *performance management* which are more widely used in a strategic context.

Literature review objective	**To identify dashboard design methods applied in strategic information security and analyze those methods for their support of SA.**

Research strategy	Keywords used:
	• Dashboard
	  ○ "Dashboard" OR "Visualization" OR "Scorecard" OR "Reporting" OR "Performance Management"
	• Information security
	  ○ "Information Security" OR "Cyber Security" OR "Cybersecurity"
	• Situation awareness
	  ○ "Situation Awareness" OR "Situational Awareness"
	• Strategic
	  ○ "Executive" OR "CEO" OR "Governance" OR "Board of Directors" OR "Director" OR "Strategy" OR "Strategic planning" OR "CISO"
	
	Source:
	EBSCO Search engine

Selection criteria	Inclusion criteria
	• The paper is either a conference paper or a journal paper.
	• The paper is peer-reviewed.
	• The paper is published in English.
	• The paper covers one of the following subjects:
	  ○ Information security strategic dashboards
	  ○ Information security dashboards supporting SA

Extraction strategy	Extraction tool: Zotero

Table 2. Literature review plan

3.1.2. Conducting the Review

Most of the papers identified by the selected keyword were not selected for the literature review as shown in table 3. Only 3.9% (2/51) of the identified papers on information security strategic dashboard are relevant to the literature review. At the non-strategic level, for information security dashboards supporting SA, 31.8% (7/22) of the identified papers have been selected.

The most common reasons for rejection are: (1) despite containing the keywords identified in table 2, the paper was unrelated to the research subject, (2) the paper did not contain enough detail on the dashboard design process to allow an adequate analysis, or (3) there was no visual representation of the dashboard, making the analysis impossible.

Subject	**Information security strategic dashboards**	**Information security dashboards supporting SA**
Papers identified by keywords	51	22
Papers identified excluding duplicates	45	21
Papers selected for review	2	7

Table 3. Papers selection process

3.1.3. SA assessment criteria

In order to answer the literature review objective, the papers have been assessed on the criteria presented in table 4. These decision rules are based on the phases of designing for SA presented in section 2.2.

SAOD phase	**Principle**	**Assessment criterion**
1. Requirements analysis	The requirements analysis is directed by the user's goals.	Is the requirement analysis method presented comparable to a GDTA? Can it be described as based on the user's goals rather than on the technology?

2. Design	**1.** Organize information around goals.	Is the information displayed in order to optimize the user's goals?
	2. Present Level 2 information directly—Support comprehension.	Is information displayed to facilitate the interpretation of progress towards the goal?
	3. Provide assistance for Level 3 SA projections.	Do the displayed indicators help assess the evolution of the situation in the future?
	4. Support global SA.	Is information relevant to all goals displayed simultaneously?
	5. Support trade-offs between goal-driven and data-driven processing.	Does the interface help the user switch between the goal prioritization mental processes and the goal achievement mental processes?
	6. Make critical cues for schema activation salient.	Have prototypical situations been identified? Is there an effort to match the displayed thresholds to the user's mental model?
	7. Take advantage of parallel processing capabilities.	Does the display maximize the amount of information as described by optimizing parallel processing as described by Wickens (2002)?
	8. Use information filtering carefully.	Is the use of filtering adequate, not interfering with understanding or projection?
3. Evaluation	Measuring the user's SA to ensure the dashboard adequacy.	Is the user's SA measured? If not, is some other type of usability evaluation conducted?

Table 4. Assessment criteria for SA

3.2. Literature review results

3.2.1. Strategic dashboards in information security

Two papers were selected regarding information security dashboards at the strategic level. This anemic body of literature highlights the fact that while information security

dashboards interest academics at the non-strategic level, they have not been studied in depth at the strategic level.

Both papers present an approach that targets concise communication, intended for an audience which wishes to see a handful of indicators summarizing the security of the organization. In one paper, the information is displayed based on the ten categories of the ES-C2M2 information security maturity model, rated on a scale of one to 5 (Adler, 2013). In the other case it displays a unique number which aggregates all the security indicators of the organization in numerical value and shows its evolution over time (Dogaheh, 2010).

Figure 4 presents author information for these papers, both of which have been published by researchers from government or private organizations, but never from academic institutions. Both instances are conference papers related to the Institute of Electrical and Electronics Engineers (IEEE).

Author	Country	University or organization	Publication title
Adler, Richard M.	United States	DecisionPath, Inc.	IEEE International Conference on Technologies for Homeland Security (HST)
Dogaheh, Morteza Ansari	Iran	Organization for Educational Research and Planning (OERP)	IEEE International Conference on Information Theory and Information Security

Figure 4. Author information

The assessment of whether the visuals presented in these papers support SA is presented in figure 5. The authors of these two articles made design choices that make it hard to make a fair assessment of some of the design principles. For that reason, these irrelevant principles have not been considered in the assessment. Principle 5, which concerns the ability to support trade-offs between goal-driven and data-driven processing is not applicable to a single chart visualization which does not distinguish between those two types of information processing. Principle 7, on the importance of optimizing the quantity of information communicated to the user, is greatly diminished due to the format, which favors simplicity at the expense of completeness of information. Finally, principle 8, which warns against the use of automatic filters to prioritize goals, is not applicable to a single chart visualization either.

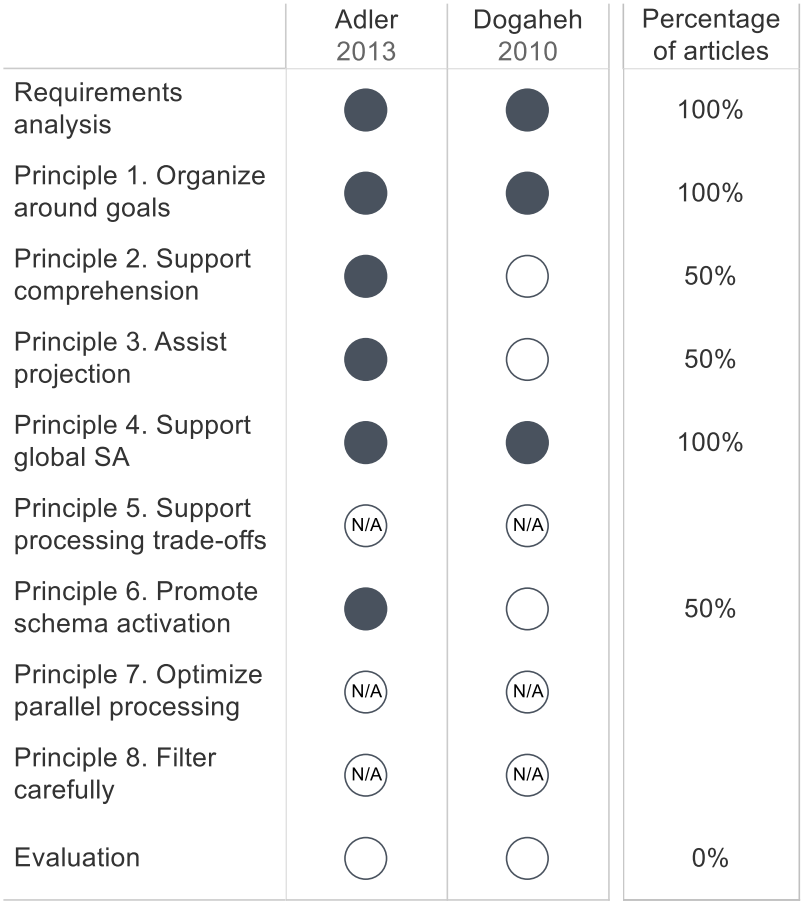

Figure 5. Papers on information security strategic dashboards for their support of SA

3.2.2. The applications of SA in information security dashboards

Considering these two papers offer limited insight into the way in which we can create dashboards that effectively support SA for information security strategic stakeholders, the subject of analysis was broadened to include papers on the use of SA in information security dashboards outside the strategic level. Figure 8 presents a summary of the seven papers identified in this body of literature. In this case, all of the eight fundamental design principles for SA could be evaluated for each paper.

As shown by figure 6, the mentioned papers have been published between 2004 and 2019, with 2 papers published in 2009 (29% of the total number of publications).

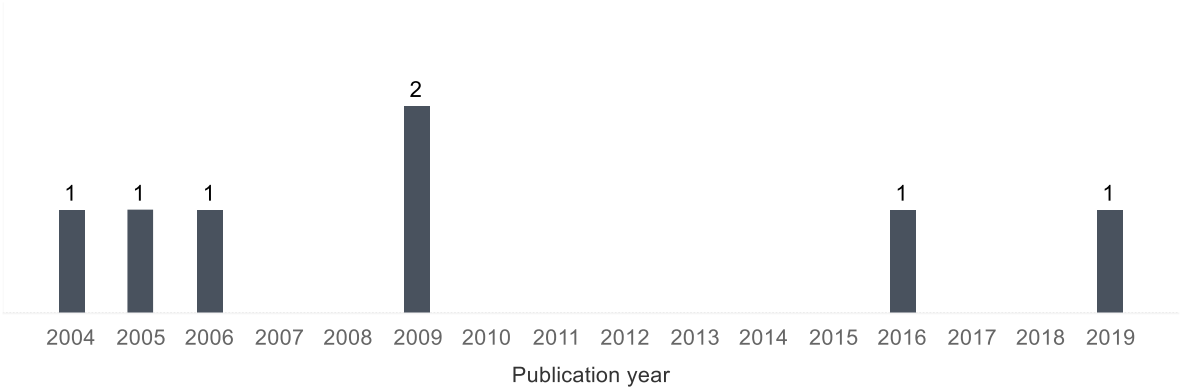

Figure 6. Number of papers published by year

Figure 7 gives additional context to the published papers. The United States has the highest number of researchers, with 19 of the 25 authors (76%). Most publications are conference papers (6 papers or 86%) and they are all connected to IEEE.. There is no obvious sign of specific interest on the subject by institutions or researchers, although two of the papers and six of the researchers are affiliated with the University of Illinois, making it the institution with most papers and most researchers on the subject. Most of the organizations are academic institutions (6 out of 8 papers or 75%), the two exceptions being the CUBRC, a private American company, and the Naval Research Academy, a Chinese government agency.

Country	University or organization	Publication title	Author	
United States	CUBRC	MILCOM - IEEE Military Communications Conference	Holsopple, Jared	1
			Sudit, Moises	1
	Rochester Institute of Technology	MILCOM - IEEE Military Communications Conference	Nusinov, Michael	1
			Yang, Shanchieh Jay	1
	University of Illinois	IEEE International Conference on Performance, Computing, and Communications	Abad, Cristina L.	1
			Lakkaraju, Kiran	1
			Xiaoxin Yin	1
			Yifan Li	1
			Yurcik, William	1
		IEEE International Workshop on Information Assurance (IWIA)	Slagell, Adam	1
			Xiaoxin Yin	1
			Yurcik, William	1
	University of Memphis	IEEE Symposium on Computational Intelligence in Cyber Security	Dasgupta, Dipankar	1
			Ferebee, Denise	1
			Lin, Yunyue	1
			Wu, Qishi	1
	University of Utah	IEEE Computer Graphics and Applications	Agutter, James	1
			Foresti, Stefano	1
			Livnat, Yarden	1
			Moon, Shaun	1
	Utah State University	IEEE Computer Graphics and Applications	Erbacher, Robert F.	1
	Total			19
Portugal	Escola Superior de Tecnologia e Gestão do Instituto Politécnico do Porto	IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity)	Carvalho, Vasco Samuel	1
			Magalhaes, Joao Paulo	1
			Polidoro, Maria Joao	1
	Total			3
China	Naval Research Academy	International Conference on Software Engineering and Service Science (ICSESS)	Zhang, Bing	1
			Zhang, Jingjing	1
			Zhang, Yuanfa	1
	Total			3
Total number of authors				25

Figure 7. Author information

The contribution of most of these papers is to create innovative ways of displaying information to provide a better SA to the user. Foresti et al. (2006) offers an innovative graph that relies on the use of visual correlations to help the user adequately detect malicious activity on the network. Xiaoxin Yin et al. (2004, 2005) describes *VisFlowConnect*, a tool that creates a graphical representation of network traffic using Parallel Axes View to grant a more complete SA to the user. These two papers lead to the same conclusions regarding their

respect of the SA design principles because they are based on the same tool in two different contexts, addressing complementary aspects of the design process. Zhang et al. (2019) suggests the use of network diagrams, which use links and nodes to represent graphically the network structure, allowing to identify key nodes and the weaker links of the network, as well as potential attacks, granting a better SA to the user. Wu et al. (2009) applies an approach that originated in biology, using algorithms to generate correlation networks in order to display network information more intuitively. These results, although they highlight the interest of using the underlying concepts of SA to improve information security, do not offer much insight into strategic information security dashboards.

On the other hand, Carvalho et al. (2016) as well as Nusinov et al. (2009) offer more integrated approaches, leading to the design of something that could be described as dashboards as defined by the research keywords. The first describes the design of a platform that collects data from multiple sources to aggregate and analyze this information, in order to display it in multiple operational dashboards. The second examines multiple visual elements and compares their ability to grant better SA to their users. It leads to a tool used to perform threat and impact assessment. While many such tools focus on the representation of security events, this visualization attempts to show the impact of these events on the organization's assets and objectives.

	Carvalho et al. 2016	Foresti et al. 2006	Nusinov et al. 2009	Wu et al. 2009	Xiaoxin Yin et al. 2004	Xiaoxin Yin et al. 2005	Zhang et al. 2019	Percentage of articles
Requirements analysis	●	●	●	○	○	○	●	57%
Principle 1. Organize around goals	●	●	○	○	○	○	●	43%
Principle 2. Support comprehension	●	●	●	●	●	●	●	100%
Principle 3. Assist projection	●	●	●	●	●	●	○	86%
Principle 4. Support global SA	●	●	●	●	○	○	●	71%
Principle 5. Support processing trade-offs	○	●	○	○	○	○	●	29%
Principle 6. Promote schema activation	○	●	●	○	●	●	○	57%
Principle 7. Optimize parallel processing	○	●	○	●	●	●	●	71%
Principle 8. Filter carefully	●	●	●	●	●	●	●	100%
Evaluation	○	●	○	○	○	○	○	14%

Figure 8. Papers on information security non-strategic dashboards for their support of SA

3.3. Implications of existing literature

One of the conclusions drawn from the literature review is that, despite the fact that the challenge to communicate efficiently security-related information at the executive level is a shared experience for many information security practitioners (Ashenden, 2008), the use of the information security strategic dashboards has seldom been studied. Although the very limited number of papers on the subject does not allow for very robust conclusions, a few general patterns can give us some insight of the research questions.

First, dashboards at the strategic level generally seem to collect requirements in a way that can be described as goal-driven (2/2), complying with the user-centered design good practices. That is not the case with non-strategic security dashboards, which would be best

described as technology-driven in almost half the cases (3/7). Secondly, the evidence of respect for the SA design principles proposed by Endsley & Jones (2011) is mixed at best, even for papers that explicitly aim to support SA. Two papers respect all the relevant SA fundamental design principles, with Adler (2013) satisfying the five design principles applicable in the strategic context. Foresti et al. (2006) respects all eight design principles but gives very limited information as to how these design choices were made and how to reproduce a similar method in a different context. In the remaining seven papers, at least two of the design principles were not met. Thirdly, only 1 paper proposes any kind of method to evaluate the usefulness of the interface, and it does not allow to reliably assess whether the interface supports the user's SA.

4. Research methodology

There are two dominant epistemologies in information technology research. While behavioral science focuses mainly on identifying “what is true”, design science first seeks to create “what is effective” (Hevner et al., 2004). These two paradigms complement each other in the creation of knowledge. The method of design science research (DSR) positions research to solve organizational problems by creating innovative artifacts. The relevance and validity of this method are summarized by conceptual framework proposed by Hevner et al. (2004). Its relevance is established through a business need in the environment, whether by people, organizations or technology. Its validity, or rigor, is established through a robust knowledge base, using theoretical foundations and existing methodologies. In turn, it contributes to the existing body of knowledge by proposing business solutions addressing real problems in the environment, enriching the basis of future research.

In order to contribute efficiently to this existing knowledge base, the current paper is positioned within two widely used research frameworks. First, the DSR knowledge contribution framework (Gregor & Hevner, 2013) provides us with a useful way to position this contribution in the existing literature by describing four types of contributions to DSR: routine design, improvement, exaptation and invention. In the current paper, the application of SAOD to information security strategic dashboards is an exaptation, that is, adapting an existing solution to a new problem.

Then, the resulting artifact can be placed in the classification of research outputs proposed by March & Smith (1995), which describes produced research artifacts as constructs, models, methods or instantiations. The current paper adapts a method to design an information security strategic dashboard supporting SA, as well as an instantiation of this method with a Canadian financial institution.

The implementation of DSR is an iterative process. Table 5 presents the process as described by Peffers et al. (2007). While the problem definition phase is stable, it is possible to return to an anterior phase as new information emerges.

Phase of DSR process (Peffers et al., 2007)	In the current paper
1. Identify the problem and justify its importance	Information security dashboards, in general, do not support SA very well. The problem is even worse at the strategic level, where almost no research on the subject has been conducted. How should a dashboard be designed in order to support the users's SA?
2. Define the objectives of a solution	The objective is to document the SAOD method to design a dashboard that supports SA of the strategic decision makers in information security, namely the CISO.
3. Design and develop a solution	The proposed solution is to apply SAOD to develop an instantiation of an information security strategic dashboard.
4. Demonstrate the solution is suitable in the context, solves the problem	The proposed solution solves the issues of the methods identified in the existing literature, allowing to consistently design dashboards that support SA.
5. Evaluate how effective and efficient the solution is to solve the problem	The usefulness of the artifact is evaluated using the SAGAT.
6. Communicate gained knowledge through professional or academic publications	The results are published as a peer-reviewed article and presented to security professionals.

Table 5. DSR Process, adapted from Peffers et al. (2007)

5. Results & Discussion

5.1. Organizational context

The method was applied as described in 2.2, leading to a dashboard mock-up for the strategic information security stakeholders of a Canadian financial institution. Since every organization is unique, we identified a few factors that impacted how we arrived at the dashboard mock-up.

Being in a context of information security in a large financial institution comes with a certain level of maturity in terms of business intelligence and analytics. However, information security reporting in this case was evolving rapidly and was not supported by a dashboard. This means that in order to complete the project, intentional steps had to be taken to manage change. Evaluating mock-ups has proven to be an excellent tool in this process.

The organization was, at the time of the research, making significant efforts to change the culture to be more data-driven. It is a very favorable context for the creation of a dashboard, and it has a major advantage: there was support, even eagerness for such a project by each stakeholder involved, which has lead to executive sponsorship as well as involvement from middle management and analysts.

5.2. Documenting the method and the instantiation

This method differs significantly from the existing literature on information security strategic dashboards presented in section 3.2.1, as detailed in table 6. There are also a few key differences between what we proposed and what is described in Endsley & Jones (2011).

These differences arise from the fact that if the original method was developed for the fast-paced context of military and aviation, a largely causal work domain, it is here applied to strategic information security in a corporate environment, a work domain with mostly intentional constraints.

SAOD Phase	Information security strategic dashboards literature	This method: Designing for SA adapted to information security strategic dashboards
Requirements Analysis	The requirements analysis is typically organized around the user's goals.	The requirements analysis is organized around the user's goals and makes explicit the elements required to support their SA by creating a GDTA.
Design	The designed dashboards do not consistently follow the 8 fundamental SA design principles as shown in figure 5.	The designed dashboards do consistently follow the 8 fundamental SA design principles, through the use of dashboard design good practices proposed by Few (2013).
Evaluation	The methods offer no process to evaluate whether the designed dashboards support the user's SA.	The method offers a process to evaluate whether the designed dashboards support the user's SA. This process is inspired by the SAGAT.

Table 6. Comparison of the proposed method to the existing literature

5.3. Phase 1: Requirements analysis

5.3.1. The Goal-Directed Task Analysis

The SA requirements analysis has been conducted through interviews with several stakeholders of the financial institution. Seven individuals, identified in appendix E, were contacted for at least 30 minutes as part of this process. The CISO was interviewed for a total of 2 hours in 3 different occurrences. Members of their team, responsible for specific security domains or initiatives were also interviewed. This process led to the development of the Goal-Decision-SA structure introduced in 2.2.1. The goal hierarchy is presented in figure 9. The complete analysis—including sub goals, decisions and SA elements—can be found in appendix A.

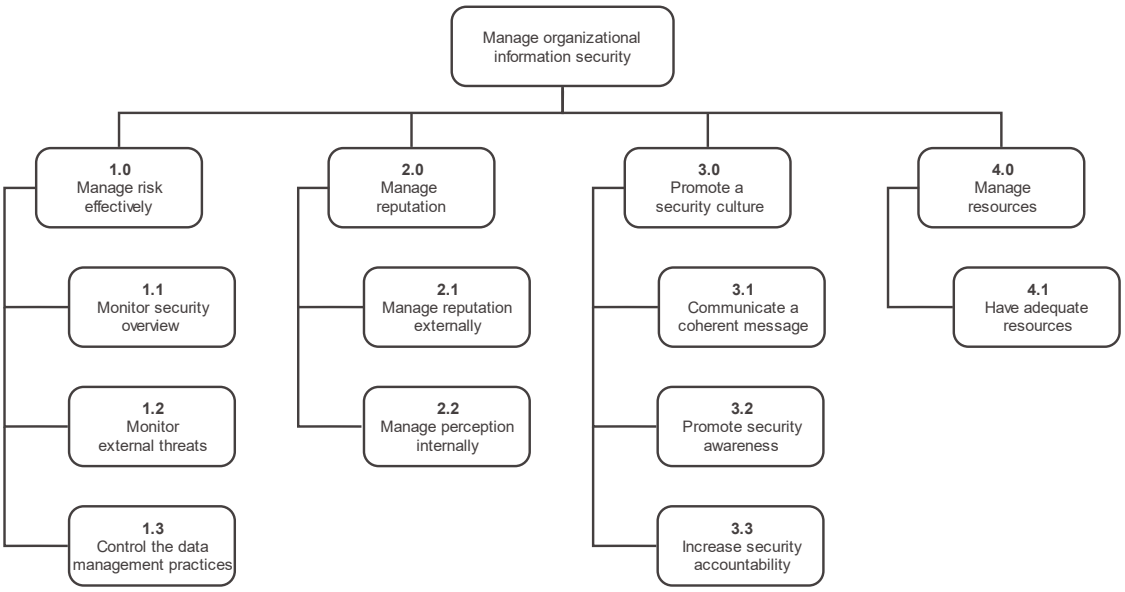

Figure 9. Goals of the CISO and their team at the targeted financial institution

The requirements analysis process that led to the GDTA was carried out iteratively; the version presented is the final version, where alignment to the dashboard mock-up is most clear. Figure 2 presents the design process as linear, completing the documentation of the requirements before the design starts. While creating our GDTA, it has been necessary to do early dashboard designs to complete the documentation of the requirements. Thus, the process was not linear. One such example of a significant change that happened after the early mock-ups is that the GDTA was considerably simplified after the user's had a visual representation. This non-linear process varies from what is presented in figure 2, and is more similar to what is proposed by ISO 9241-210:2019 Human-centered design for interactive systems (ISO, 2019), which explicitly encourages the usage of the design artifact to specify the context of use and requirements.

Challenge 1: The GDTA is limited as a communication tool; some of the informational requirements were changed after stakeholders viewed the mock-ups.

Through this process, the documentation of requirements that we achieved is useful, allowing us to document the needs of the users that enables iterative conception and is the basis of the subsequent evaluation of the design. However, it could be more thorough. The depth of analysis obtained in some GDTA's presented in the literature could not be achieved in our context due to the nature of the work domain at hand. Operational environments tend to be causal work domains, mostly limited by constraints that cannot be violated. Strategic environments, on the other hand, tend to be intentional work domains, where the constraints are much more subjective, stemming from conventions or values (Naikar, 2013; Rasmussen et al., 1994). An operational information security stakeholder might ensure the adequate application of the established organizational password policies. A strategic information security stakeholder might need to decide what this policy is. The constraints on these two goals are very different in their nature, thus having an impact that could not be mitigated on the produced GDTA.

Challenge 2: Strategic environments tend to be more subjective and to consist of a handful of stakeholders who are short on time, which leads to a less thorough GDTA.

The goal-driven nature of the GDTA has sometimes led to informational requirements that could not be met in the organizational context. An example of this is the measure of customer perception for information security. Despite being an interesting concept, it was deemed too difficult to measure adequately to have tangible value for the organization in the dashboard.

Challenge 3: Informational requirements obtained from a goal-driven analysis sometimes cannot be met because they are not measurable in the organizational context.

Then there also were some of the informational requirements that were better met by tools other than the dashboard. This is exemplified by the choice to remove financial information from the dashboard. This type of information, especially in a financial institution, is crucial for the CISO. However, there are already reporting mechanisms that meet this

informational need, therefore including high-level summaries in the dashboard would have had little benefit in this context.

Challenge 4: Informational requirements obtained from a goal-driven analysis are sometimes better met by means other than the proposed dashboard.

These two challenges were mitigated by the use of early dashboard mock-ups to help define the user's requirements. Given these limitations, the GDTA produced for strategic goals will not be as broadly applicable or as objective as it would be for operational goals. However, this GDTA is still valuable because it fulfills its general goal of providing insight into the mental model of the CISO and other strategic information security stakeholders.

5.3.2. Metrics and indicators

The GDTA was the cornerstone of the process used to identify the right indicators for the dashboard. While this structured way of documenting requirements ensures that the indicators identified are relevant to the user, there are many other factors to consider before making the final selection.

At this point, it seems relevant to distinguish the indicator from the metric. While a metric measures a business process, an indicator measures the execution of the business strategy (Eckerson, 2011). Typically, an indicator is a metric for which a target has been set to provide insight into the achievement of goals. With this in mind, the dashboard displays indicators, which have been built based on the selected metrics.

Many authors in information security discuss information security metrics. Brotby & Hinson (2016) provide a comprehensive analysis of all the major authors on the subject, extensively documenting an impressive number of metrics that could be used. Jaquith (2007) is particularly interesting, offering a business-centric rather than security-centric metric selection process like most other authors.

These information security best practices can be aligned with the user's goal, creating a list of metrics that are both robust and useful. That leads to the third element that had a central importance in the choice of metrics: the specific context of the organization. In our case, an example of this is the use of the five functions of the NIST Cybersecurity Framework (NIST, 2018) to organize the security overview section. Since the organization is currently assessing its security posture with this framework, it would be counterproductive to display such information based, for example, on the ISO 27002 (ISO, 2013) nomenclature, even though it could be a valid choice for other organizations.

Then, as the dashboard starts to take shape, identifying the number of indicators that should be displayed can become contentious. In the literature, there is no agreed upon rule on the number of indicators that can be displayed. A common way to think about it is that dashboards should contain as few indicators as possible but as many as necessary. Eckerson (2011) uses 12 distinct indicators as a rule of thumb. Jaquith (2007) suggests that more than 25 indicators in a scorecard such as the one we present becomes problematic. Tufte (1983), however, has argued that as long as it is displayed properly, more information is better than less information, and that information density should be maximized, within reason. We argue that our dashboard, containing 30 distinct indicators, satisfices this criterion of maximizing information density within reason.

The choice of the best indicators is one of the ever-challenging aspects of dashboard design, and there is room for improvement in the process we used. Eckerson (2011) gives a more thorough insight into this problem. Some elements, such as the inclusion of leading and lagging indicators, have not been considered in the design process. While leading indicators measure the business activities that influence the outcomes, lagging indicators measure the outcome itself (Eckerson, 2011). A robust performance management program contains both types of indicators.

5.4. Phase 2: Design

After several iterations, a final mock-up was produced. It is presented in figure 10. This dashboard mock-up contains no real data.

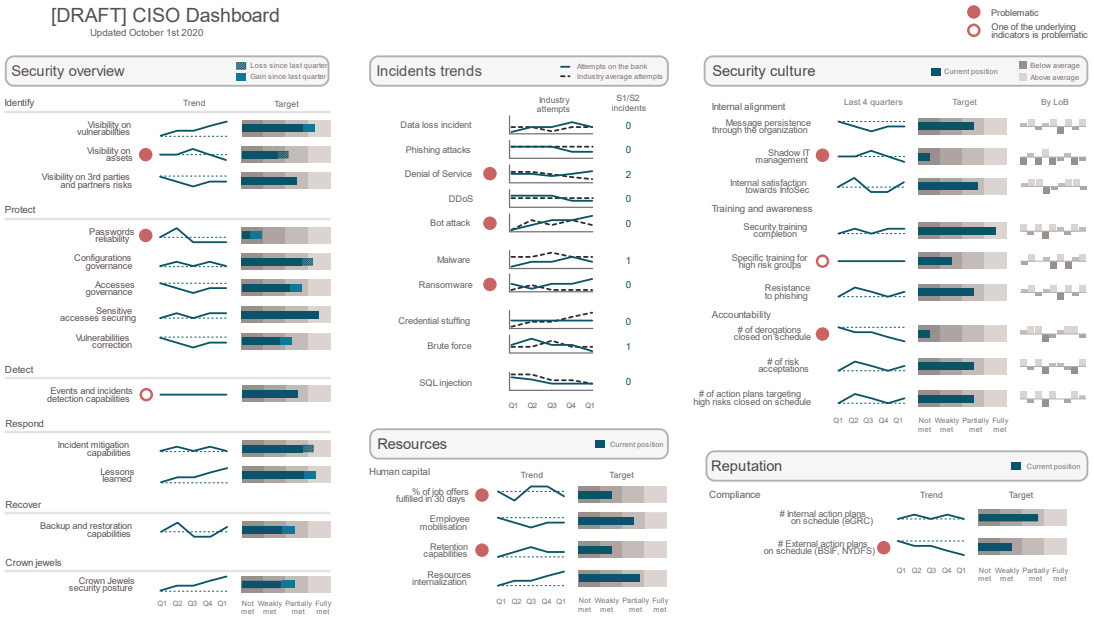

Figure 10. Final dashboard mock-up

The iterative nature of the process was key in the evolution of the design. A good example of these iterative changes is the “internal alignment” section of the dashboard, presented in figure 11.

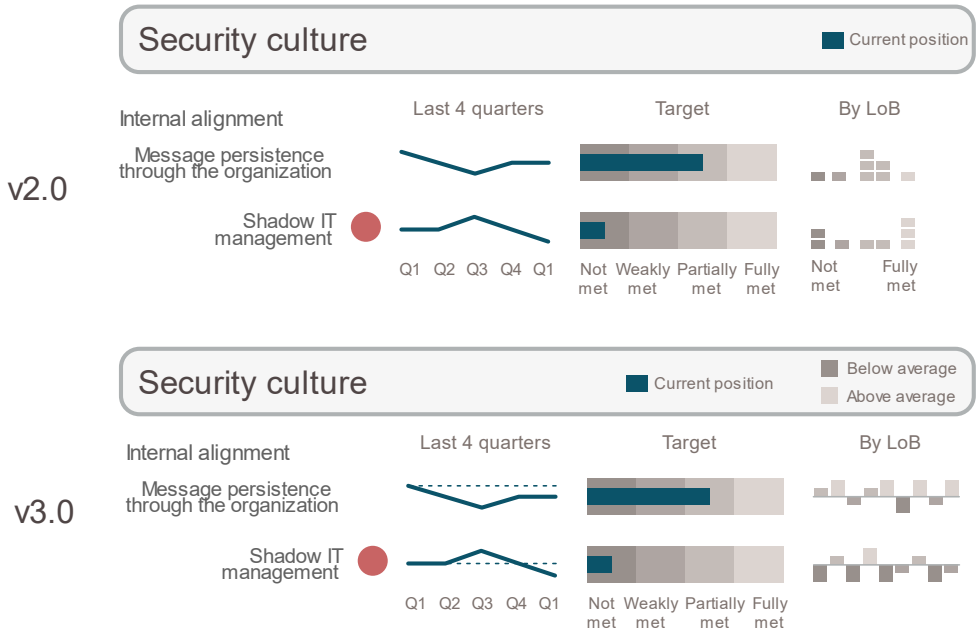

Figure 11. Evolution of dashboard components

First, the addition of the dotted reference line to the trend in v3.0 makes it easier for the user to compare performance to the previous year. Secondly, the overhauled distribution of the performance by lines of business (By LoB) makes it easier to have an integrated perspective. In v3.0, it is much easier to identify a line of business with weaknesses on both message persistence and shadow IT management, as an example. There are many more changes that came with each version, this evolution is documented in appendix B.

The way in which the eight design principles have been applied, detailed in table 7, was heavily influenced by Few (2013). This explains some of our design choices, such as the considerable effort to stick to a single page, the use of greyscales as often as possible and the use of graphs that are highly space efficient such as the bullet graph and the sparkline.

	Principle	How the principle was applied
1	Organize information around goals	The dashboard is divided into sections according to the goals of the CISO, the information presented is therefore organized around goals.
2	Present Level 2 information directly—Support comprehension	By displaying the relevant context for the measures with a target and a measure of the distribution of the results, the user's comprehension is directly supported.
3	Provide assistance for Level 3 SA projections	By showing trends, where appropriate, it is easier for the user to interpret what is likely to happen next.
4	Support global SA	By adopting a one page monitoring view, the dashboard supports global SA.
5	Support trade-offs between goal-driven and data-driven processing	By organizing the information by goals and displaying relevant information on a single page, both processing mechanisms are supported with minimal user effort.
6	Make critical cues for schema activation salient	Considering the ever-changing environment at the strategic level, identifying prototypical situations is much less relevant. However, the inclusion of alert indicators and acceptability thresholds are critical cues for schema activation since they become links to the user's mental schemas.
7	Take advantage of parallel processing capabilities	The parallel processing capabilities of the user are optimized through the mechanisms proposed by (Wickens, 2002). The use of both visual channels is favored by the use of a single page and the inclusion of highly visible red alert indicators. Then, the various codes of information processing are supported through the use of a single page and the choice of graphs; mostly sparklines and bullet graph (Few, 2013).
8	Use information filtering carefully	The dashboard does not contain any filters.

Table 7. Application of the fundamental SA design principles

After going through this process, we conclude that the challenges met in this phase are not specific to SAOD. One could argue that by using only Few (2013) as a reference guide for designing dashboards, one could easily meet the eight fundamental SA design principles. That being said, designing dashboards is a challenging process in and of itself.

First, back and forth was required to define what level of detail would most adequately meet the informational needs of the strategic stakeholders . Too much detail would mean it is not possible to achieve all the goals in one page, too few details would mean that the dashboard does not allow efficient decisions to be made. As the first mock-ups were too detailed, it was decided to display most of the information in the form of higher-level aggregated indicators. The construction of these higher-level indicators has the advantage of making it possible to keep all the metrics that we had identified. However, it also can hide the intricacies of the data if not done properly. To limit this risk, these groupings of indicators were produced iteratively with the key stakeholders. Although robustness of these constructs has not been empirically proven, users generally did not have any issues with them throughout the testing. Two examples of such grouped indicators are shown in figure 12.

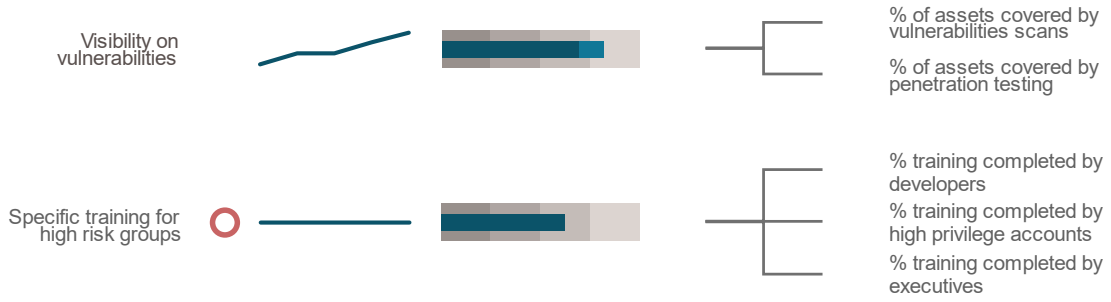

Figure 12. Examples of aggregate indicators

Another challenge consisted of figuring out what situations should lead to display an alert indicator. In our dashboard, alert indicators are the principal tool to prioritize information and are crucial to the activation of the user's mental schemas. After discussions with the stakeholders, robust rules have been defined to display a primary alert (full red circle), as well as a less intrusive, secondary alert (empty red circle) if any of the underlying indicators is problematic but that issue did not manifest itself at the higher level.

Finally, data availability in the organizational context means that in the current version, data is updated on a quarterly basis. With fewer constraints on data availability, monthly or weekly data could be more relevant to the CISO.

5.5. Phase 3: Evaluation

In order to assess whether the designed dashboard provides a complete and accurate SA to its users in a real-world scenario, a set of queries on the SA elements identified in the GDTA was prepared. The process was loosely based on the SAGAT, having for goal to measure the user's SA by assessing its components: perception, understanding and capability for projection. It led to the SAGAT Queries in appendix C.

It important to note that significant adaptations have been made to tailor the method to the context. The SAGAT method requires a complex dynamic user interface in order to limit the impact the measurement on the user's attentional resources. This constraint exists so that the measurement interferes as little as possible with the user's ability to maintain the SA previously obtained. If reaching a complete SA quickly is relevant at the strategic level of organization, we argue that maintaining that SA is not nearly as important as it is in many operational contexts, where the interface is updated in real time in order for the user to be able to take decisions instantly. Moreover, a less complex and easier to implement evaluation solution is more pragmatic, allowing evaluation to be integrated earlier in the design process and enabling faster iterations subsequently.

Challenge 5: The SAGAT as described by Endsley (1988) requires a complex evaluation apparatus to limit interference with the user's attentional resources.

Challenge 6: The importance of having a sustained, uninterrupted SA is not as important in a strategic context as it is in an operational context.

For these two reasons, we chose to conduct the evaluation as follows. Three versions of the dashboard were created with different values. The questions were displayed at the same time as the mock-up, not one after the other. The users answered the written questions orally, before choosing when to display the next question. At unpredictable intervals, the values displayed changed between the three datasets. A note was made when the user expressed confusion about specific aspects of the dashboard.

An unintended benefit of having the users answer orally is that some tend to go into detail about the information that led to their answer, giving deeper insight into their decisions, resembling in some ways using verbal protocols to perform the evaluation. However, these departures from the empirically tested SAGAT limit the reliability and validity of our test. Most of the stakeholders that were involved in the design of the GDTA were selected to evaluate the mock-up dashboard. Ultimately the evaluation was conducted with 6 participants, with the CISO being involved on two occasions.

Referring to the mock-ups in appendix B, the evaluation was carried out as follows: All the iterations up to version 1.0 inclusively were evaluated in a relatively unstructured, informal context. Iterations 2 and 3 were evaluated using the SAGAT queries and the described methodology.

The results of the evaluation process have been carefully documented. Three notable results have been identified in the data presented in appendix D. First, the dashboard is complex and can be overwhelming upon the first look. During their first few minutes of contact with the dashboard, users gave disproportionally unexpected answers, whereas for users who were familiar with the dashboard consistently gave more expected answers. Secondly, the time to answer the questions appears to be roughly randomly distributed. There is no clear trend in questions that always required more time to answer, or users that consistently took more time to answer than others. There are no clear trends in the difference between the test of v2.0 and v3.0 either.

There are also multiple methodological limitations that make the value of these results questionable. Since the process took place with strategic stakeholders with limited availability, only 3 or 4 evaluators participated to each iteration, which limits the thoroughness of the evaluation.

Challenge 7: Strategic environments tend to be made up of a handful of busy stakeholders, leading to a less thorough evaluation.

Then, our methodology, although inspired by the SAGAT, is not conducted as described in section 2.2.3. Consequently, even though the SAGAT has been empirically tested for reliability and validity, our testing methodology has not. Due to the questions being answered orally, there is no clear way to interpret the time to answer; longer answers might be more complete or might have required additional effort to get to the answer. This information was stored in the comments of the test, allowing to identify visualizations that were harder to read. The SAGAT also allows to compare different iterations of a design artifact. Our testing methodology does not, since the stakeholders that participate in the testing change between iterations.

This evaluation of the dashboard is undeniably useful to determine whether the design adequately meets the needs of the stakeholders. It also has the benefit of pressuring users to spend time with the design and learn how to use it, reducing the training costs and improving the chances of project success (ISO, 2019).

6. Conclusion

In this paper, we present a method in three phases that makes it possible to create information security strategic dashboards that consistently support SA. This dashboard, in turn, should enable strategic decision makers in information security, such as the CISO, to take better decisions.

The method we describe addresses two deficiencies we identified in the literature. First, there is no existing literature on the use of SA in information security dashboards at the strategic level; our method is centered on a strategic process. Secondly, the examples of such dashboards at the operational level were not consistently successful in their attempt to support users' SA; we describe a method that reaches this result reliably.

To do so, we propose an exaptation, based on the method of SAOD, adapted to the context of information security strategic dashboards. We also document the design journey, giving insight into how the method can be used for practitioners by developing a dashboard mock-up with a Canadian financial institution. This case study allows to confirm the usefulness of the detailed method in organizational context, by including (1) the GDTA, a framework to document the user's requirement that is systematic and comprehensive, leading to a dashboard that is helpful in the decision-making process, (2) an example of application of the design guidelines proposed by Endsley & Jones (2011) in order to create a dashboard that supports the user's SA, and (3) an evaluation methodology inspired by the SAGAT, that is both thorough and flexible, able to give good insights into what should be improved in the dashboard while allowing for rapid iterations in the design.

6.1. Future work

We believe this method can be improved in three key ways, that could be the source of future research.

First, the GDTA, although undeniably useful in the definition of the needs, requires a very thorough documentation process that might not be suitable to every business context.

The Goal-Question-Metric approach from software engineering (Basili et al., 1994), offers some of the benefits of the GDTA while being less detailed and might be worth looking into. The balanced scorecard framework (Kaplan & Norton, 1992), commonly used in strategic performance management, might also deliver additional gain since it will most likely be already familiar to executive stakeholders.

Secondly, the visual components used in the dashboard have been realized using the widely accepted good practices of user-centered design. The next step towards optimally supporting the user's SA could be to look into ecological interface design (Vicente & Rasmussen, 1992), which might have a significant impact by making explicit the causal relations between the indicators.

Thirdly, the evaluation method was undeniably relevant in our context, and could be described as the most useful contribution of the method. However, it is significantly different from the SAGAT, its reliability and validity still need to be empirically established.

6.2. Acknowledgements

This work was supported by Mitacs Accelerate [Grant Numbers FRA45554, FRA45555]; and Cybereco. These organizations had no role in the study design, the collection, analysis and interpretation of the results, the writing of the paper or the decision to submit the article for publication.

7. Bibliography

Adler, R. M. (2013). A dynamic capability maturity model for improving cyber security. *2013 IEEE International Conference on Technologies for Homeland Security (HST)*, 230–235. https://doi.org/10.1109/THS.2013.6699005

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report*, *13*(4), 195–201. https://doi.org/10.1016/j.istr.2008.10.006

Basili, V. R., Caldiera, G., & Rombach, H. D. (1994). The Goals Question Metric Approach. *Encyclopedia of Software Engineering*, 10.

Brotby, W. K., & Hinson, G. (2016). *PRAGMATIC Security Metrics: Applying Metametrics to Information Security*. Auerbach Publications.

Carvalho, V. S., Polidoro, M. J., & Magalhaes, J. P. (2016). OwlSight: Platform for Real-Time Detection and Visualization of Cyber Threats. *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, 61–66. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.73

Dogaheh, M. A. (2010). Introducing a framework for security measurements. *2010 IEEE International Conference on Information Theory and Information Security*, 638–641. https://doi.org/10.1109/ICITIS.2010.5689505

Eckerson, W. (2011). *Performance Dashboards: Measuring, Monitoring, and Managing Your Business*. John Wiley & Sons.

Endsley, M. R. (1995a). Measurement of Situation Awareness in Dynamic Systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 65–84. https://doi.org/10.1518/001872095779049499

Endsley, M. R. (1995b). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors*, *37*(1), 32–64.

Endsley, M. R. (1988). Situation awareness global assessment technique (SAGAT). *Proceedings of the IEEE 1988 National Aerospace and Electronics Conference*, 789–795 vol.3. https://doi.org/10.1109/NAECON.1988.195097

Endsley, M. R., Bolstad, C., Jones, D., & Riley, J. (2003). Situation Awareness Oriented Design: From User's Cognitive Requirements to Creating Effective Supporting Technologies. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *47*.

Endsley, M. R., & Jones, D. G. (2011). *Designing for Situation Awareness: An Approach to User-Centered Design* (Second Edition). CRC Press.

Few, S. (2013). *Information Dashboard Design: Displaying Data for At-a-Glance Monitoring* (Second Edition). Analytics Press.

Foresti, S., Agutter, J., Livnat, Y., Moon, S., & Erbacher, R. (2006). Visual correlation of network alerts. *IEEE Computer Graphics and Applications*, *26*(2), 48–59. https://doi.org/10.1109/MCG.2006.49

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness – A systematic review of the literature. *Computers & Security*, *46*, 18–31.

Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*, *37*(2), 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105.

ISACA. (2012). *COBIT 5: A business framework for the governance and management of enterprise IT: an ISACA® framework*. ISACA.

ISO. (2013). *ISO 27002:2013 Information technology, Security techniques, Code of practice for information security controls*.

ISO. (2019). *ISO 9241-210:2019 Ergonomics of human–system interaction, part 210: Human-centred design for interactive systems*.

Jaquith, A. (2007). *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Addison-Wesley Professional.

Kaplan, R. S., & Norton, D. P. (1992). The Balanced Scorecard—Measures that Drive Performance. *Harvard Business Review*, *January-February*, 71–79.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251–266.

Naikar, N. (2013). *Work Domain Analysis: Concepts, Guidelines, and Cases*. CRC Press.

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

Nusinov, M., Yang, S. J., Holsopple, J., & Sudit, M. (2009). ViSAw: Visualizing threat and impact assessment for enhanced situation awareness. *MILCOM 2009 - 2009 IEEE*

Military Communications Conference, 1–7. https://doi.org/10.1109/MILCOM.2009.5380104

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77.

Rasmussen, J., Pejtersen, A. M., & Goodstein, L. P. (1994). *Cognitive Systems Engineering* (1st edition). Wiley-Interscience.

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *British Journal of Management*, *14*(3), 207–222. https://doi.org/10.1111/1467-8551.00375

Tufte, E. R. (1983). *The visual display of quantitative information* (Vol. 2, Issue 9). Graphics press Cheshire, CT.

Vicente, K. J., & Rasmussen, J. (1992). Ecological interface design: Theoretical foundations. *IEEE Transactions on Systems, Man, and Cybernetics*, *22*(4), 589–606. https://doi.org/10.1109/21.156574

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A Situation Awareness Model for Information Security Risk Management. *Computers & Security*, *44*, 1–15.

Wickens, C. D. (2002). Multiple resources and performance prediction. *Theoretical Issues in Ergonomics Science*, *3*(2), 159–177. https://doi.org/10.1080/14639220210123806

Wu, Q., Ferebee, D., Lin, Y., & Dasgupta, D. (2009). Visualization of security events using an efficient correlation technique. *2009 IEEE Symposium on Computational*

Intelligence in Cyber Security, 61–68. https://doi.org/10.1109/CICYBS.2009.4925091

Xiaoxin Yin, Yurcik, W., & Slagell, A. (2005). The Design of VisFlowConnect-IP: A Link Analysis System for IP Security Situational Awareness. *Third IEEE International Workshop on Information Assurance (IWIA'05)*, 141–153. https://doi.org/10.1109/IWIA.2005.17

Xiaoxin Yin, Yurcik, W., Yifan Li, Lakkaraju, K., & Abad, C. (2004). VisFlowConnect: Providing security situational awareness by visualizing network traffic flows. *IEEE International Conference on Performance, Computing, and Communications, 2004*, 601–607. https://doi.org/10.1109/PCCC.2004.1395108

Zhang, Y., Zhang, J., & Zhang, B. (2019). Visual Analysis of Cybersecurity Situational Awareness. *2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS)*, 685–688. https://doi.org/10.1109/ICSESS47205.2019.9040716

8. Appendices

8.1. Appendix A: Goal-Directed Task Analysis

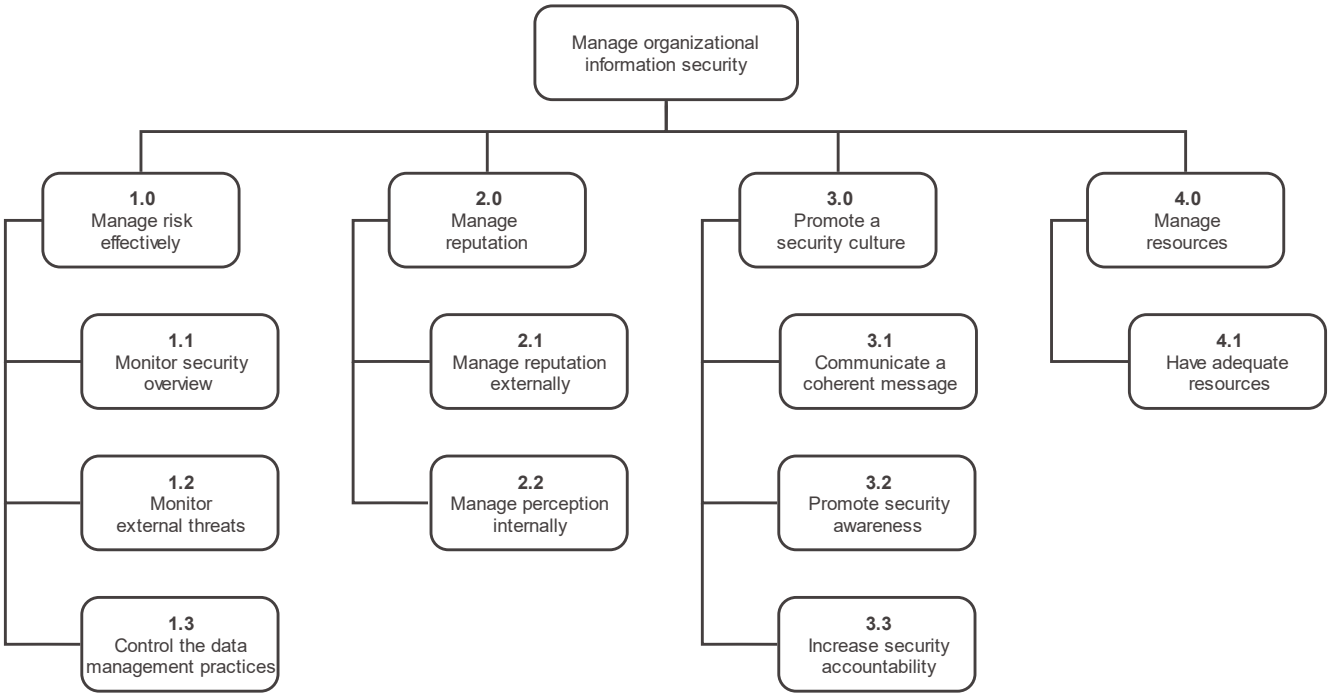

Figure A.1.

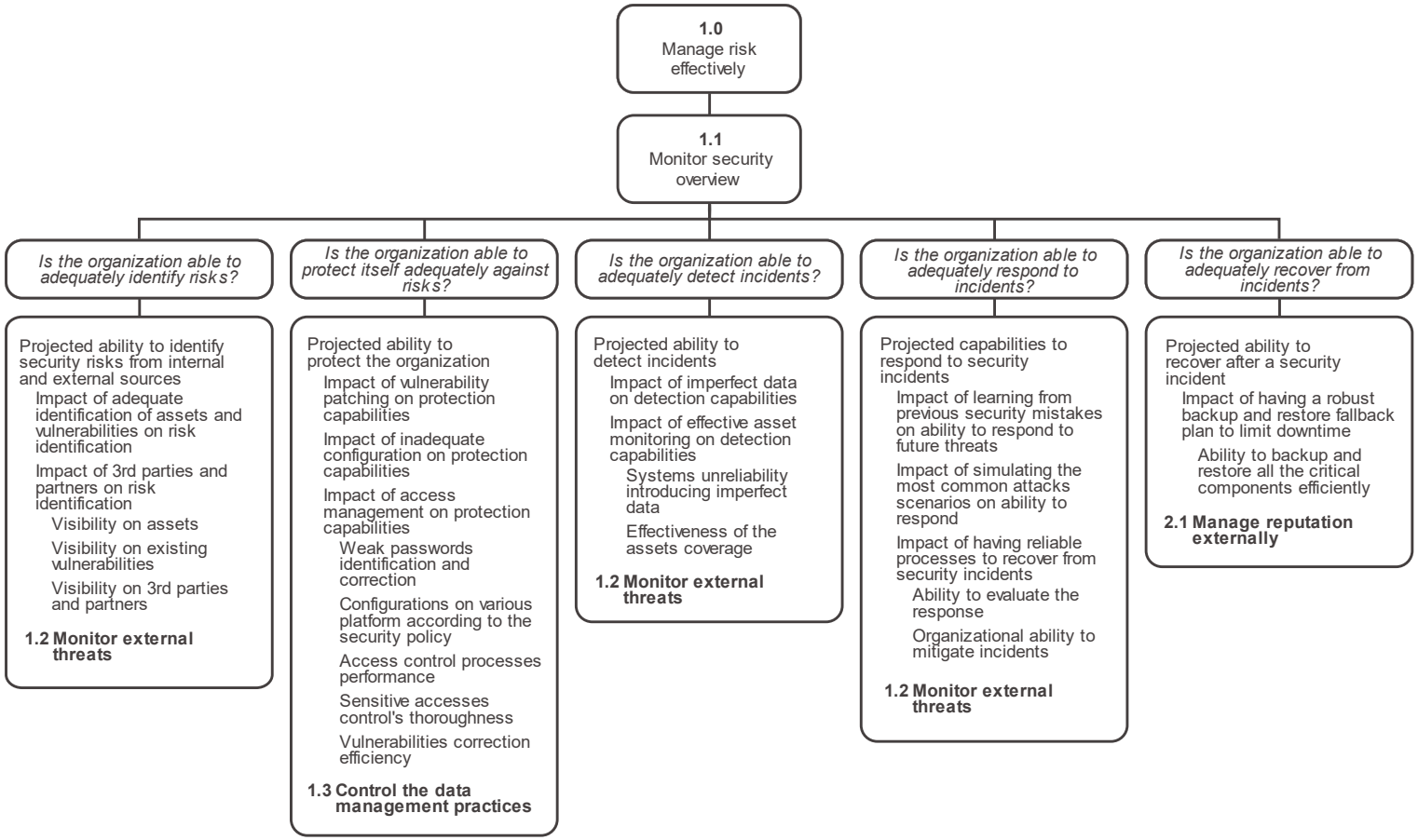
1.0
Manage risk effectively
1.1
Monitor security overview
Is the organization able to adequately identify risks?
Is the organization able to protect itself adequately against risks?
Is the organization able to adequately detect incidents?
Is the organization able to adequately respond to incidents?
Is the organization able to adequately recover from incidents?
Projected ability to identify security risks from internal and external sources
Impact of adequate identification of assets and vulnerabilities on risk identification
Impact of 3rd parties and partners on risk identification
Visibility on assets
Visibility on existing vulnerabilities
Visibility on 3rd parties and partners
1.2 Monitor external threats
Projected ability to protect the organization
Impact of vulnerability patching on protection capabilities
Impact of inadequate configuration on protection capabilities
Impact of access management on protection capabilities
Weak passwords identification and correction
Configurations on various platform according to the security policy
Access control processes performance
Sensitive accesses control's thoroughness
Vulnerabilities correction efficiency
1.3 Control the data management practices
Projected ability to detect incidents
Impact of imperfect data on detection capabilities
Impact of effective asset monitoring on detection capabilities
Systems unreliability introducing imperfect data
Effectiveness of the assets coverage
1.2 Monitor external threats
Projected capabilities to respond to security incidents
Impact of learning from previous security mistakes on ability to respond to future threats
Impact of simulating the most common attacks scenarios on ability to respond
Impact of having reliable processes to recover from security incidents
Ability to evaluate the response
Organizational ability to mitigate incidents
1.2 Monitor external threats
Projected ability to recover after a security incident
Impact of having a robust backup and restore fallback plan to limit downtime
Ability to backup and restore all the critical components efficiently
2.1 Manage reputation externally

Figure A.2.

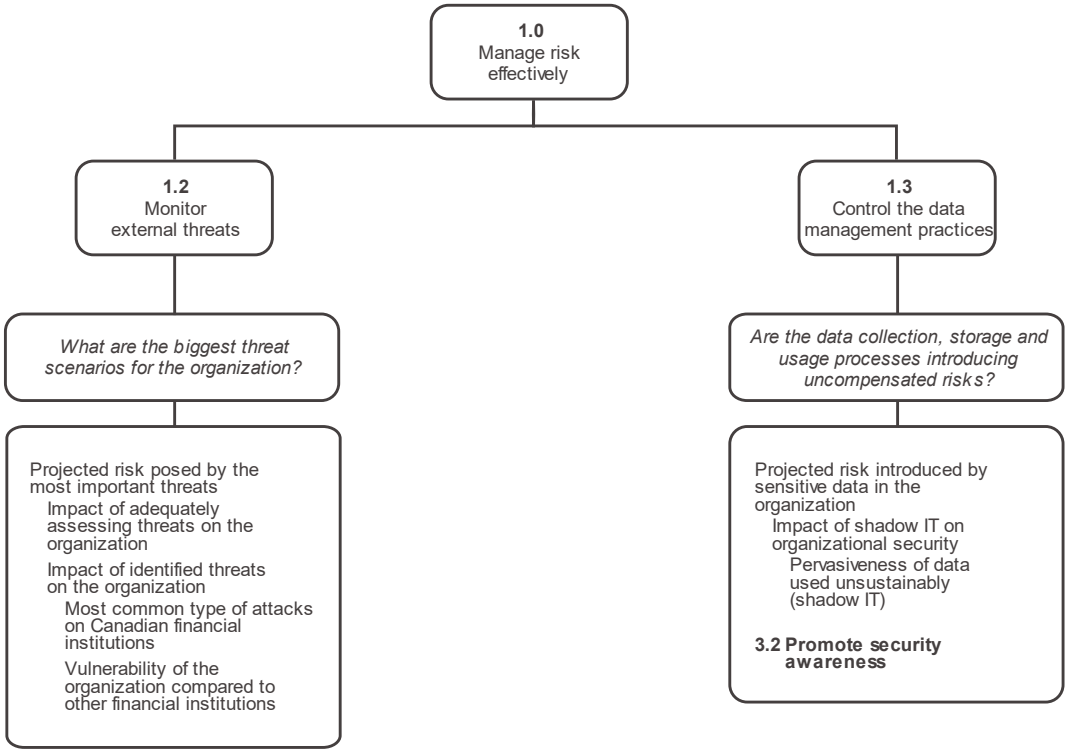
1.0
Manage risk effectively
1.2
Monitor external threats
1.3
Control the data management practices
What are the biggest threat scenarios for the organization?
Are the data collection, storage and usage processes introducing uncompensated risks?
Projected risk posed by the most important threats
Impact of adequately assessing threats on the organization
Impact of identified threats on the organization
Most common type of attacks on Canadian financial institutions
Vulnerability of the organization compared to other financial institutions
Projected risk introduced by sensitive data in the organization
Impact of shadow IT on organizational security
Pervasiveness of data used unsustainably (shadow IT)
3.2 Promote security awareness

Figure A.3.

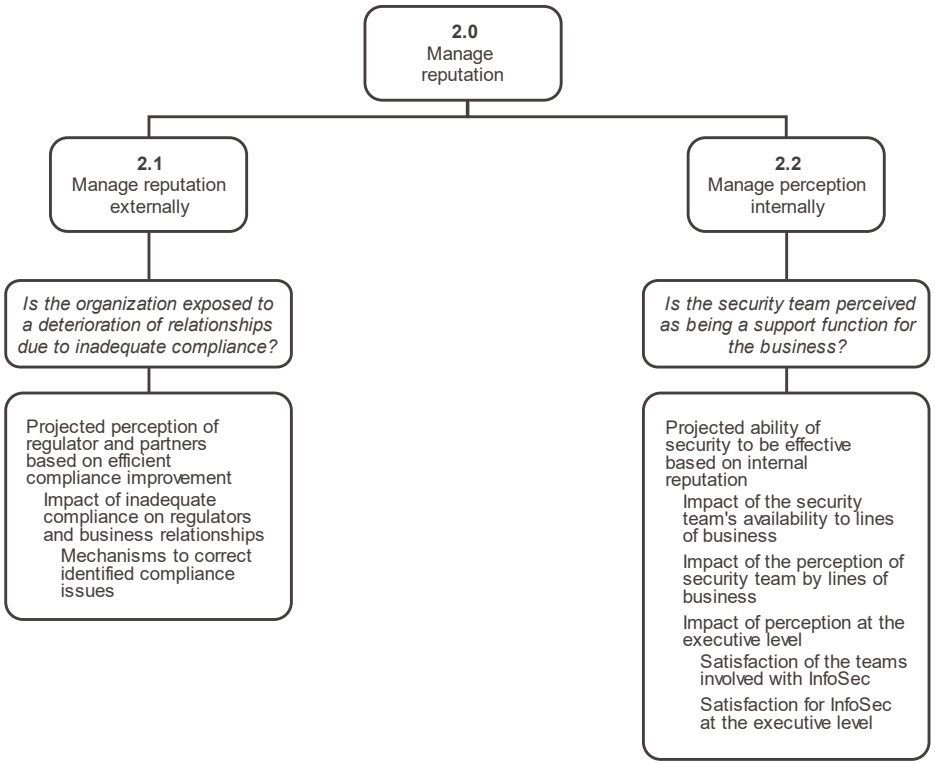
2.0
Manage reputation
2.1
Manage reputation externally
2.2
Manage perception internally
Is the organization exposed to a deterioration of relationships due to inadequate compliance?
Is the security team perceived as being a support function for the business?
Projected perception of regulator and partners based on efficient compliance improvement
Impact of inadequate compliance on regulators and business relationships
Mechanisms to correct identified compliance issues
Projected ability of security to be effective based on internal reputation
Impact of the security team's availability to lines of business
Impact of the perception of security team by lines of business
Impact of perception at the executive level
Satisfaction of the teams involved with InfoSec
Satisfaction for InfoSec at the executive level

Figure A.4.

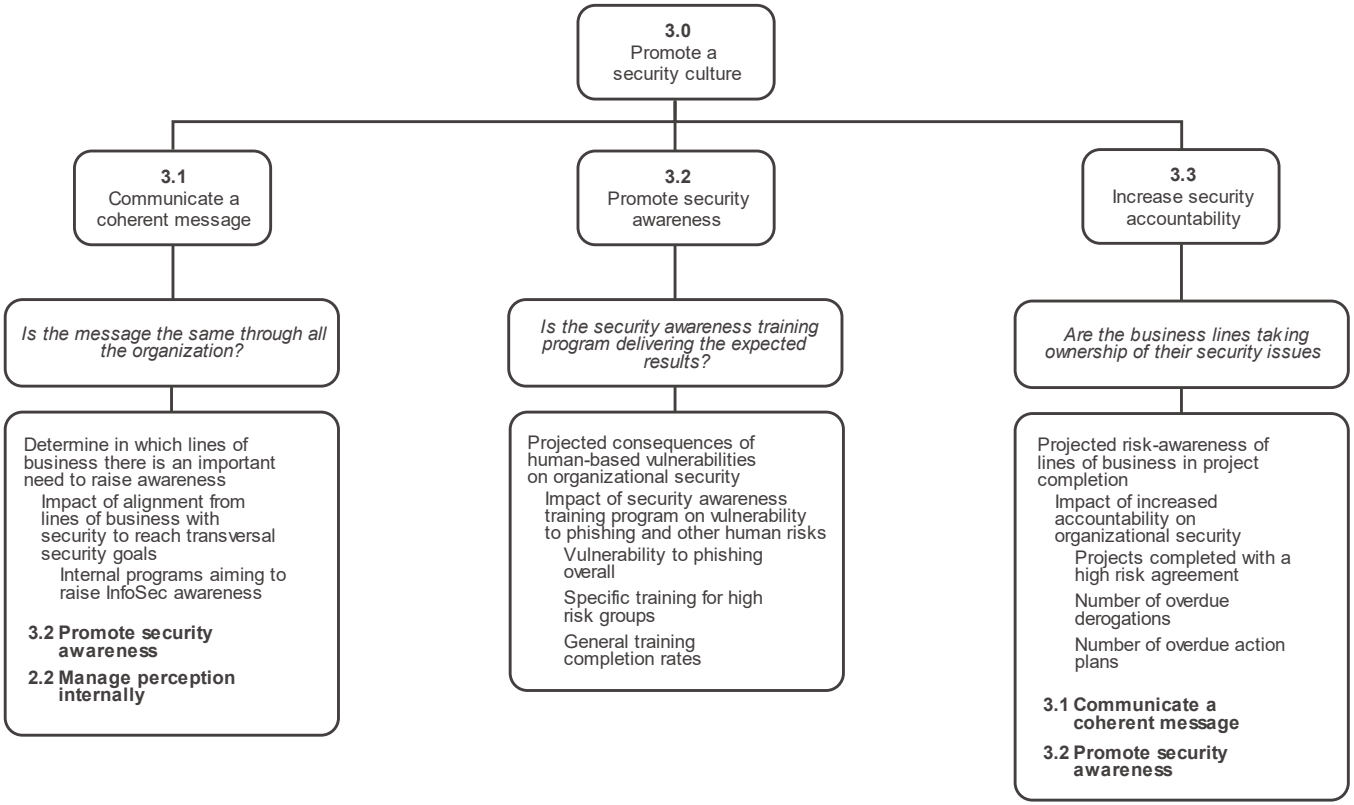
3.0
Promote a security culture
3.1
Communicate a coherent message
3.2
Promote security awareness
3.3
Increase security accountability
Is the message the same through all the organization?
Is the security awareness training program delivering the expected results?
Are the business lines taking ownership of their security issues
Determine in which lines of business there is an important need to raise awareness
Impact of alignment from lines of business with security to reach transversal security goals
Internal programs aiming to raise InfoSec awareness
3.2 Promote security awareness
2.2 Manage perception internally
Projected consequences of human-based vulnerabilities on organizational security
Impact of security awareness training program on vulnerability to phishing and other human risks
Vulnerability to phishing overall
Specific training for high risk groups
General training completion rates
Projected risk-awareness of lines of business in project completion
Impact of increased accountability on organizational security
Projects completed with a high risk agreement
Number of overdue derogations
Number of overdue action plans
3.1 Communicate a coherent message
3.2 Promote security awareness

Figure A.5.

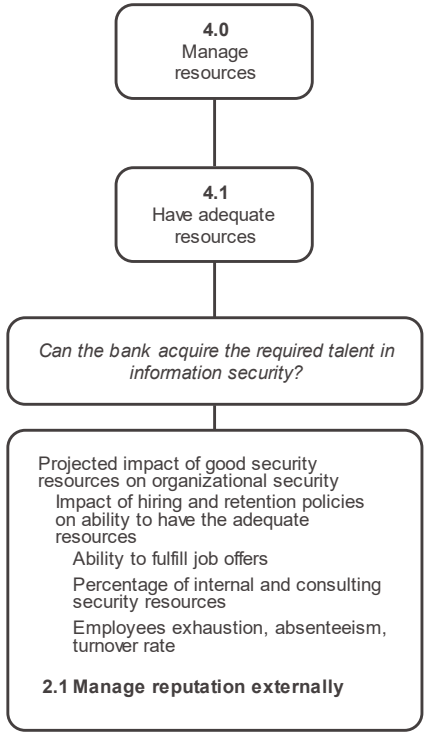
4.0
Manage resources
4.1
Have adequate resources
Can the bank acquire the required talent in information security?
Projected impact of good security resources on organizational security
Impact of hiring and retention policies on ability to have the adequate resources
Ability to fulfill job offers
Percentage of internal and consulting security resources
Employees exhaustion, absenteeism, turnover rate
2.1 Manage reputation externally

Figure A.6.

8.2. Appendix B: Evolution of the mock-up

The dashboard mock-ups presented in the paper are not based on real data.

8.2.1. Strategic Information Security Dashboard v1.0

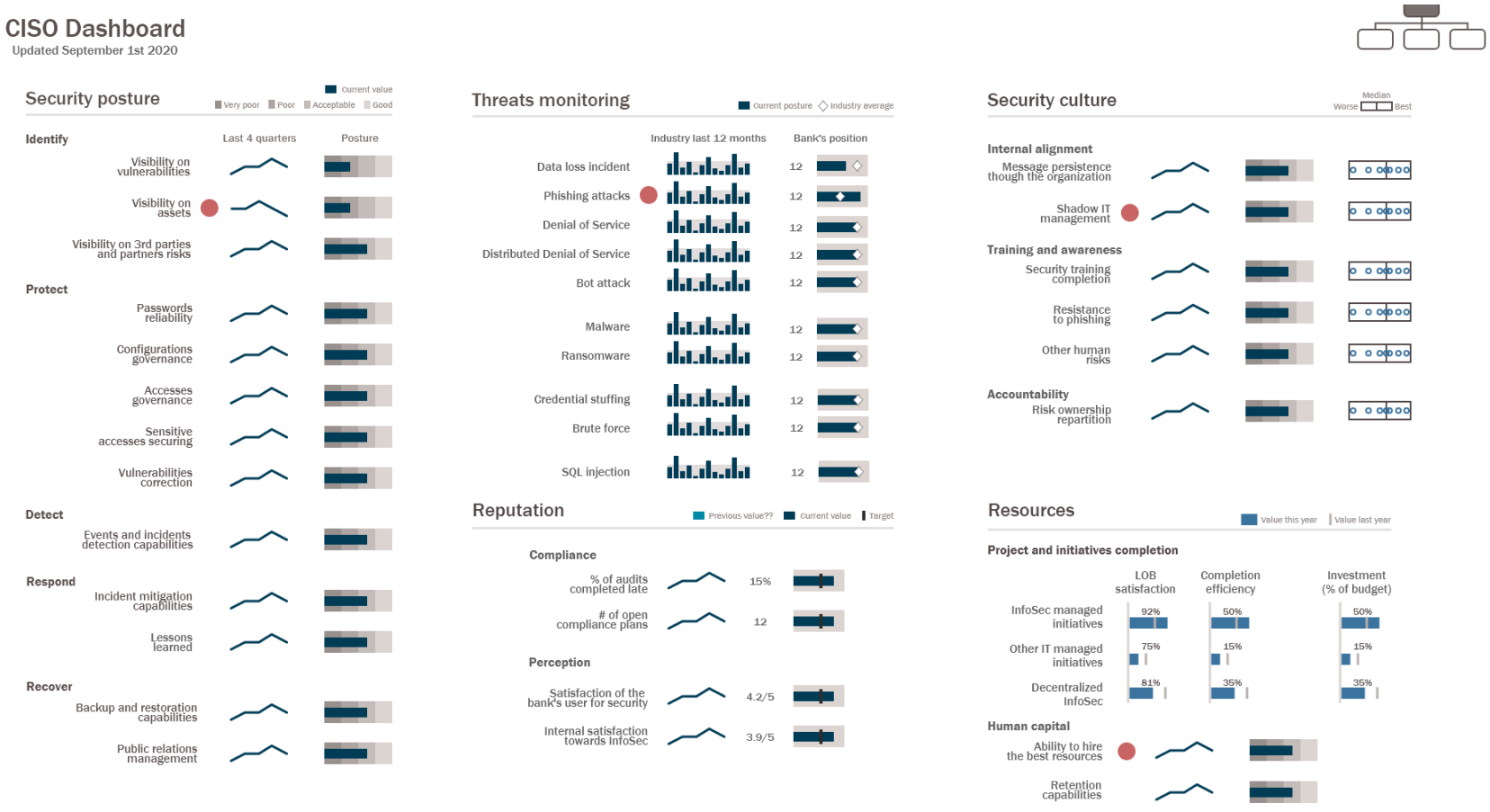

Figure B.1.

8.2.2. Strategic Information Security Dashboard v2.0

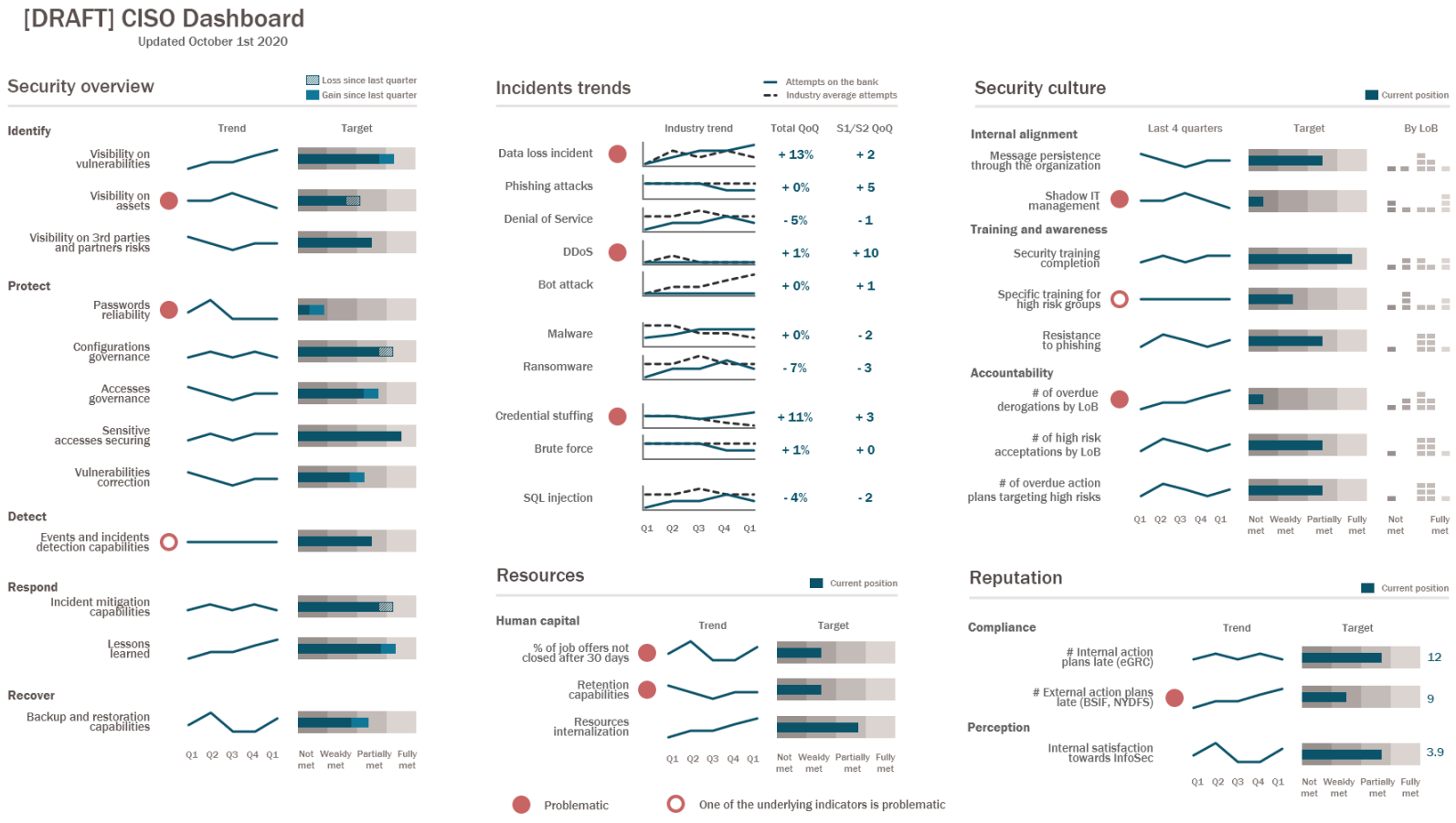

Figure B.2.

8.2.3. Strategic Information Security Dashboard v3.0

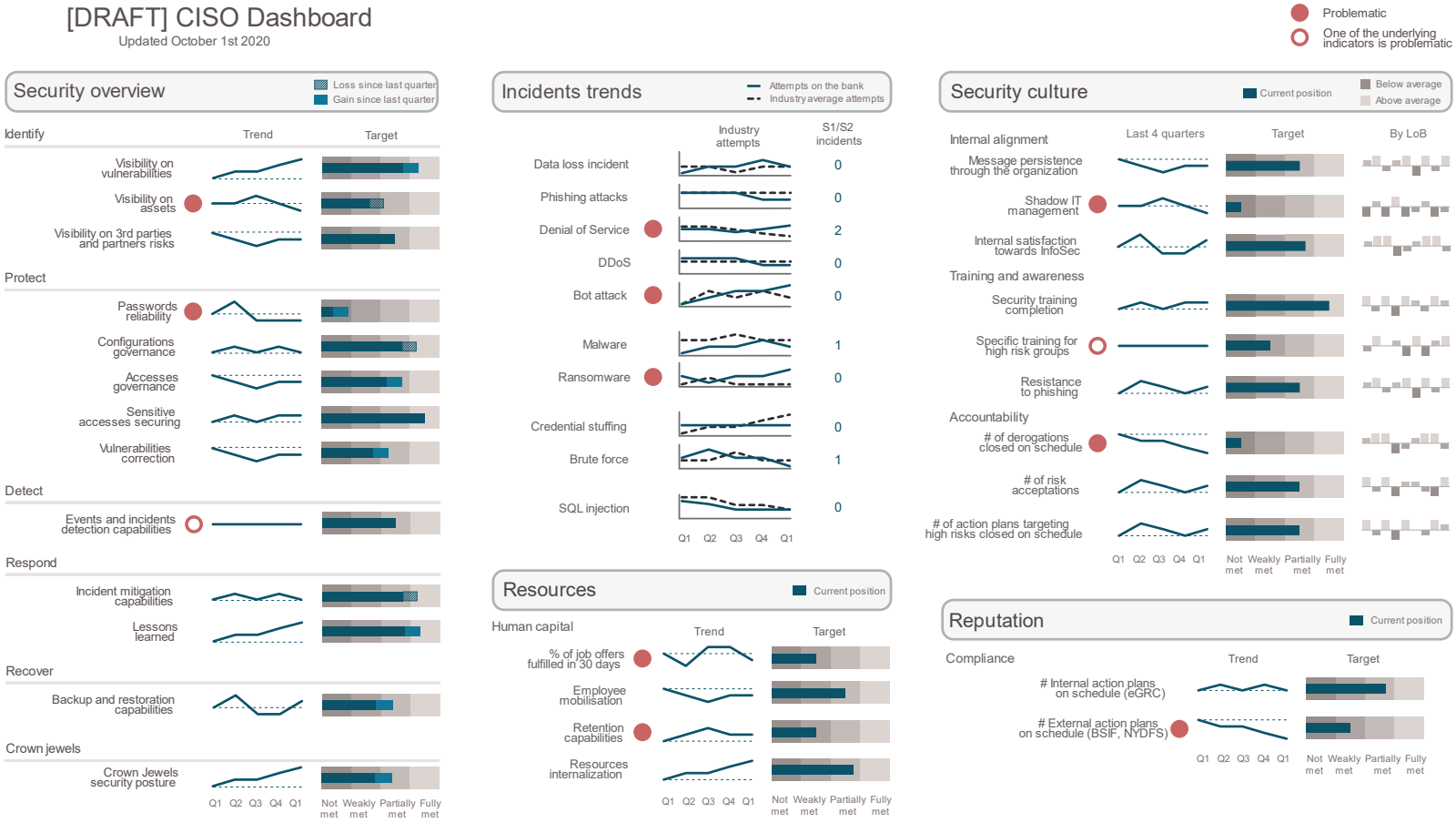

Figure B.3.

8.3. Appendix C: SAGAT Queries

#	Sub-goal	SA Level	Item
1	1.1	Perception	Is the target for vulnerabilities correction currently met?
2	3.2	Perception	Is the training completion target for high risk groups currently met?
3	4.1	Perception	Is the target for hiring capabilities currently met?
4	1.2	Perception	What are the incident types for which the bank is significantly above the industry average?
5	3.2	Perception	Which line of business has the lowest resistance to phishing?
6	1.1	Perception	Have the event and incident detection capabilities improved over the last year?
7	1.1	Comprehension	Are the bank's current identification capabilities impacted by 3rd parties and partners?
8	1.1	Comprehension	How worrisome are each of the five functions of the security overview?
9	1.2	Comprehension	What can be concluded from the trend in incidents?
10	1.3	Comprehension	Is the information security message being communicated adequately through the organization?
11	2.1	Comprehension	Does the current compliance status have a negative impact on our relationship with regulators?
12	2.2	Comprehension	Is information security perceived internally as an enabler for the business?
13	3.1	Comprehension	Is there a line of business where the security message persistence is problematic?
14	3.2	Comprehension	Is the training program currently useful to mitigate risks?
15	3.3	Comprehension	Are the lines of business taking ownership of information security?
16	4.1	Comprehension	Is the bank currently able to staff information security initiatives adequately?

17	1.1	Projection	Considering the trend in the security overview, which elements are expected to be problematic in the close future?
18	1.2	Projection	Which incident types are most likely to occur in the next weeks?
19	1.3	Projection	Are the efforts to mitigate shadow IT progressing adequately?
20	2.1	Projection	Is relationship with regulators likely to be impacted by inadequate compliance in the short term?
21	2.2	Projection	Is the perception of information security as an enabler of business initiatives likely to improve in the short term?
22	3.1	Projection	Which lines of business will require additional efforts to promote information security awareness?
23	3.2	Projection	Is there an imminent need to make changes to the training and awareness program?
24	3.3	Projection	Is the trend in lines of business taking accountability for information security generally positive?
25	4.1	Projection	If the percentage of job offers not closed after 30 days keeps increasing, when is it expected to become a serious issue?

Table C.1.

8.4. Appendix D: Evaluation results

	Test 1							
	User 1 (FC)		User 2 (FC)		User 3 (FC)		User 4 (FC)	
Q	Expect. answer?	Time (s)	Expect. answer?	Time (s)	Expect. answer?	Time (s)*	Expect. answer?	Time (s)
1	Y	7	S	58	S	NA	Y	20
2	S	11	S	54	Y	NA	Y	9
3	S	30	Y	17	Y	NA	Y	24
4	S	18	S	33	N	NA	N	19
5	S	24	Y	23	N	NA	N	27
6	Y	10	Y	49	N	NA	S	28
7	Y	16	Y	13	N	NA	Y	26
8	Y	10	Y	75	Y	NA	Y	29
9	Y	9	Y	38	Y	NA	Y	80
10	Y	55	Y	15	Y	NA	Y	98
11	Y	35	Y	13	Y	NA	Y	8
12	Y	40	Y	5	Y	NA	N	34
13	Y	13	Y	16	Y	NA	Y	29
14	Y	55	Y	21	Y	NA	Y	40
15	Y	47	Y	29	Y	NA	Y	7
16	Y	51	S	14	Y	NA	Y	36
17	Y	46	Y	19	Y	NA	Y	28
18	Y	27	Y	14	N	NA	Y	37
19	Y	26	Y	24	Y	NA	Y	25
20	N	23	Y	17	Y	NA	Y	60
21	Y	15	Y	9	Y	NA	N	12
22	Y	26	Y	26	Y	NA	Y	30
23	Y	27	Y	25	Y	NA	Y	11
24	Y	45	Y	51	Y	NA	Y	25
25	Y	34	S	55	Y	NA	S	36
Total		700		713		NA		778

Table D.1.

Y = Yes, S = Somewhat, N = No

FC = First contact with the dashboard

* There was an issue with the recording of this interview, the measure of the times to answer was not reliable.

Test 2						
	User 1		User 2		User 3	
Question	Expected answer?	Time to answer (s)	Expected answer?	Time to answer (s)	Expected answer?	Time to answer (s)
1	Y	11	Y	6	Y	48
2	Y	12	Y	7	Y	17
3	Y	11	Y	16	Y	30
4	Y	13	Y	17	Y	31
5	Y	18	Y	15	Y	7
6	N	21	Y	21	Y	12
7	Y	28	Y	15	Y	18
8	Y	80	Y	84	Y	34
9	Y	70	Y	55	Y	26
10	Y	23	Y	10	Y	37
11	Y	50	Y	24	Y	24
12	Y	19	Y	23	Y	32
13	Y	13	Y	3	Y	9
14	Y	29	Y	14	Y	58
15	Y	44	Y	56	Y	22
16	Y	23	Y	32	Y	31
17	Y	19	Y	70	Y	29
18	Y	20	Y	5	Y	22
19	Y	38	Y	16	Y	30
20	Y	9	Y	25	Y	36
21	Y	12	Y	17	Y	44
22	Y	5	Y	24	Y	27
23	Y	44	Y	42	Y	32
24	Y	41	Y	121	Y	31
25	Y	43	Y	40	Y	42
Total		696		758		729

Table D.2.

Y = Yes, S = Somewhat, N = No

	Total Time	Average time per question	Std dev per question	Median time per question	Minimum time per question	Maximum time per question
Test 1	700	28	15.0	26	7	55
	713	28.52	18.0	23	5	75
	778	31.12	20.7	28	7	98
Average	730.3					
Std dev	34.1					
Test 2	696	27.84	18.8	21	5	80
	758	30.32	27.5	21	3	121
	729	29.16	11.6	30	7	58
Average	727.7					
Std dev	25.3					

Table D.3.

8.5. Appendix E: Respondents

Participant	Role	Experience in IT and information security	Sex	Participation
P1	Senior Manager, Information Security	Over 10 years	F	RE
P2	Senior Advisor, Information Security	Over 10 years	M	RE
P3	Director, Information Security	Over 15 years	M	RE
P4	Enterprise IT Architect	Over 20 years	M	RE
P5	Senior Advisor, Information Security	Over 10 years	M	R
P6	Senior Advisor, Information Security	Over 10 years	M	R
P7	Security Service Owner	Over 5 years	M	R
P8	Chief Information Security Officer	Over 15 years	F	RE
P9	Director, Information Security	Over 5 years	M	E

Table D. 4.

R: Participation to the documentation of the requirements

E: Participation to the evaluation of the mock-ups

RE: Participation to both the documentation of the requirements and the evaluation of the mock-ups