NOVA IMS
Information Management School

MGI

Mestrado em Gestão de Informação
Master Program in Information Management

Cybersecurity Planning Insight :
CSCD (Cyber Security and Cyber Defense) Control Framework For Strategic Direction and Governance

MAHMUDUL HASAN
M20190507

Dissertation presented as partial requirement for obtaining the Master’s degree in Information Management, with a specialization in Information systems and Technologies Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

NOVA Information Management School

Instituto Superior de Estatística e Gestão de Informação

Universidade Nova de Lisboa

CYBERSECURITY PLANNING INSIGHT: CSCD (CYBER SECURITY AND CYBER DEFENSE) CONTROL FRAMEWORK FOR STRATEGIC DIRECTION AND GOVERNANCE

BY

MAHMUDUL HASAN

Dissertation presented as partial requirement for obtaining the Master's degree in Information Management, with a specialization in Information systems and Technologies Management

Supervisor: Vitor Santos

July 2021

ACKNOWLEDGMENTS

First of all, I would like to take the opportunity to express my gratitude to Professor Dr. Vitor Duarte dos Santos of NOVA IMS for the guidance and support throughout this research. Since from the very first day, his adequate time and regular status update meeting help me to make a proper strategy and plan for this research to finish on time. Most importantly, the motivation and inspiration that I got from my Professor was the key for me. To be honest, I have learned so many things from the Professor, which will be an asset for me for my further studies. Thank you, sir, for believing in my capability to finish this diverse research work.

I would also like to thank some authors and publishers of the research paper and frameworks for giving me access to gather data, especially during this pandemic context; it was very important and meaningful for me. Nevertheless, it helped to get a more precise understanding of the field of research and the constructive insight to contribute to a more advanced and tech-driven topic.

Likewise, I would like to thank my employer BNP Paribas for allowing me to continue my thesis besides full-time work. Significantly, the support and inspiration I got from Goncalo Pina my hierarchical manager (CIO, BNP Paribas CIB, Portugal) and my functional manager Jeremy Sanson (Head of IT strategy, BNP Paribas headquarter, France) were helped me to concentrate much on my thesis besides office work.

Lastly, but not least, I would like to thank my family (mother, sister, and brother-in-law) for giving me continuous motivation. Besides, my friends, colleagues, and the well-experienced faculty from NOVA IMS always gave me good suggestions and shared their experiences which helped me to do my thesis work. Since from the very first day, I started with a dream to complete my graduation from NOVA IMS; eventually, I am very close to that incredible journey. Thank you, NOVA IMS, and all of my teachers, for the light of knowledge that I achieved from you will be a vital breakthrough for my further career and study.

ABSTRACT

In this recent time, the importance of cybersecurity and cyber defense is sky-high. Everyone uses different devices, IT infrastructures, and applications for various purposes at school, office, home, hospitals everywhere. With the enlightenment of technology, the nature of cyber-attack has been changed dramatically, and that is why the number of cyber-attacks have been increased. Enterprises face billions of Euros loss from such incidents; even the data loss and operational hazard may have a devastating impact not only on the service, security, privacy, brand image but also upon overall business. A constrictive and realistic CSCD (cyber security and cyber defense) strategy along with the proper implementation of it, can safeguard the enterprises and strongly from cyber attacks. In this paper, we prepare an improved CSCD control framework based on several hundreds of scientific papers and frameworks. Moreover, we identify different aspects and strategic elements by holistic CSCD control risk assessment and data analysis for preparing CSCD strategy and planning of different levels of organizations to maintain effective CSCD governance and cyber resilience.

KEYWORDS

Strategical Cybersecurity Defense; Unauthorised Access; Cyber Vigilance; Cyber Resilience; Cyber Governance

INDEX

1. Introduction 12

1.1 Background and Problem Identification 12

1.2 Problem Justification 13

1.3 Research Question 14

1.4 Study Objectives 14

1.5 Study Relevance and Importance 15

2. Literature Review 17

2.1 Strategic elements for Cyber Security and Cyber Defense: 17

2.1.1 Variants of Cyber Attack 17

2.1.2 Recent Cyber Threats 18

2.1.3 Business Centric Strategic Elements 19

2.1.4 Cyber Security and Cyber Defense (CSCD) Governance 19

2.1.5 Cyber Security and Defense Intelligence: 21

2.1.6 Strategic Cyber threat intelligence (CTI) : 22

2.2 Cyber defense model strategic approach: 23

2.3 Cyber Security Strategic Pillars: 26

3. Conceptual Research Model 28

4. Research Methodology: 30

5. CSCD Control FramEwork For Strategic Guideline and Planning 33

5.1 Assumption 33

5.2 Study and analyze major Cybersecurity and Cyber Defense Framework and ......
scientific research papers 34

5.3 CSCD Control Framework Concept 36

5.4 CSCD Control Framework Fundamental 37

5.5 Framework Implementation. 38

5.5.1 CSCD Governance 40

5.6 CSCD Framework Component 41

5.6.1 CSCD Control Criteria 42

5.6.1.5 CSCD Framework Function: 45

5.7 CSCD Control Baseline 57

5.7.1. Security Strategy and Planning Control Family 57

5.7.2 Policy, Business Continuity, and compliance 58

5.7.3. Hardware Asset Management 59
5.7.4. Software Asset Management... 61
5.7.5. Vulnerability Management 63
5.7.6. Privileged Accounts Management.. 65
5.7.7. Identity, Access, and Authentication Management 67
5.7.8. Configuration Management (Hardware, Software, Mobile device,.............. laptop, Workstation, servers, IoT, etc.).. 72
5.7.9. Maintenance, Monitoring, and Log Management 73
5.7.10. Email, Browser, and Web Protections 75
5.7.11. Malware Defense Management.. 76
5.7.12. Limitation and Control of Network Ports, Protocols, and Services......... 78
5.7.13. Network Device Security (Firewall, Routers, Switch and etc.)................ 79
5.7.14. Network Defense 80
5.7.15. Wireless Access Control 83
5.7.16. Data Protection, Recovery, and Backup 84
5.7.17. Application Software Security 86
5.7.18. Risk Assessment and Management 88
5.7.19. Incident Response and Management 89
5.7.20. Penetration Tests and Red Team Exercises 90
5.7.21. Security Awareness and Training 91
5.7.22. External Service Management 92
5.8 Risk level Landscape based on RMM Level 93
5.8.1. Risk Level Landscape for Micro to Small Enterprise................................ 94
5.8.2. Risk Level Landscape for Small to Medium Enterprise............................ 94
5.8.3. Risk Level Landscape for Medium to Large Enterprise............................ 95
5.8.4. Risk Level Landscape for Large to Super Large Enterprise 95
5.9. Overall Risk Landscape all types of Enterprises Based on Risk Score:.............. 96
5.10. CSCD High Risk Parent Control Family landscape based on RMM Level: 97
5.11. Diversity of Sophistication Level on RMM Level Enterprise........................... 98
6.0 Conclusion 100
6.1 Synthesis of the research 100
6.2 Limitations of the Work...101
6.3 Next steps and Future Work..102
References 103
Annexes...112

LIST OF FIGURES

Figure 1: Different variants of Cyber Attacks (Stiawan et al., 2017).....................................18
Figure 2: Kill chain model for cybersecurity and defense (Hutchins et al., 2011) 21
Figure 3: Cyber capability defense model (Kolini & Janczewski, 2015). 24
Figure 4: Cyber capability passive defense model (Kolini & Janczewski, 2015) 24
Figure 5: Cyber capability active defense model (Kolini & Janczewski, 2015) 25
Figure 6: Cyber capability collaborative defense model (Kolini & Janczewski, 2015) 25
Figure 7: Cyber capability defense actors (Kolini & Janczewski, 2015)..................................26
Figure 8: Research Methodology Overview 31
Figure 9: IDEAL model elaboration (Poore, 2006). 39
Figure 10: IDEAL model framework implementation (Poore, 2006). 39
Figure 11: CSCD governance level (Gashgari et al., 2017)..41
Figure 12: Roles, Activities, and Relationships interaction for CSCD governance 41
Figure 13: NIST cybersecurity framework function (Barrett, 2018)......................................45
Figure 14: Risk assessment within risk management process (NIST, 2011)...........................49
Figure 15: Organization-wide risk management (Kelley, 2014). 50
Figure 16: Information security model, the CIA triad (Al-Far et al., 2019).............................53
Figure 17: RL Landscape (Micro to Small) 94
Figure 18: RL Illustration (Micro to Small)...94
Figure 19: RL Landscape (Small to Medium) 95
Figure 20: RL Illustration (Small to Medium)...95
Figure 21: RL Landscape (Medium to Large) 95
Figure 22: RL Illustration (Medium to Large)...95
Figure 23: RL Landscape (Large to Super Large) 96
Figure 24: RL Illustration (Large to Super Large)...96
Figure 25: Risk Score Landscape of parent controls based on RMM Level 97
Figure 26: CSCD High Risk Parent Control Family landscape based on RMM Level 98
Figure 27: Sophistication level on micro to small 98
Figure 28: Sophistication level on Small to Medium..98
Figure 29: Sophistication level on Medium to large 99
Figure 30: Sophistication level on Large to Super Large 99

LIST OF TABLES

Table 1: Conceptual model of research....28
Table 2: Analized framework and research papers....36
Table 3: CSCD Parent Control Family 43
Table 4: IT Asset Type 45
Table 5: CSCD control sophistication level (Union & For, 2016)....47
Table 6: CSCD Risk Management maturity Level enterprise category....48
Table 7: CSCD Risk Tolerance Level 51
Table 8: Process of measuring impact and likelihood....52
Table 9: Impact and likelihood score calculation....52
Table 10: CSCD Impact criteria (CSA, 2019) (Cronin, 2018), (Thayer et al., 2013) 56
Table 11: Likelihood criteria (CSA, 2019) (Cronin, 2018) (Thayer et al., 2013) 57
Table 12: Security Strategy and Planning Control Family 58
Table 13: Policy, Business Continuity, and compliance....59
Table 14: Hardware Asset Management 61
Table 15: Software Asset Management 63
Table 16: Vulnerability Management....65
Table 17: Identity, Access, and Authentication Management 71
Table 18: Configuration Management 73
Table 19: Maintenance, Monitoring, and Log Management....75
Table 20: Email, Browser, and Web Protections 76
Table 21: Malware Defense Management 78
Table 22: Limitation and Control of Network Ports, Protocols, and Services 79
Table 23: Network Device Security (Firewall, Routers, Switch and etc.) 80
Table 24: Network Defense 83
Table 25: Wireless Access Control 84
Table 26: Data Protection, Recovery, and Backup....86
Table 27: Application Software Security control 88
Table 28: Risk Assessment and Management 89
Table 29: Incident Response and Management control 90
Table 30: Penetration Tests and Red Team Exercises control....91
Table 31: Security Awareness and Training....92
Table 32: External Service Management control....93

LIST OF ABBREVIATIONS AND ACRONYMS

AI	Artificial Intelligence
BOT	Build Operator Transfer
C2	Command and Control
CD	Cyber Defense
CMA	Cyber Maturity Assessment
CNA	Computer Network Attack
CNE	Computer network espionage
CRM	Customer Relationship Management
CSCD	Cyber Security and Cyber Defense
CTI	Cyber Threat intelligence
DDos	Distributed Denial of Service
ERP	Enterprise Resource planning
GDPR	General Data Protection Regulation
IoT	Internet of Things
ITSP	Information Technology Strategic Plan
NDA	Non Disclosing Agreement
RMM	Risk Management Maturity
OT	Operational Technology
SEMR	Smart Medical Devices and Electronic Medical Records
RL	Risk Level
SC	Sub Control

GLOSSARY

- **Botnet**: A botnet is a number of Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform Distributed Denial-of-Service (DDoS) attacks, steal data, send spam, and allow the attacker to access the device and its connection.
- **Defense-in-depth:** Defense in depth is a concept used in Information security in which multiple layers of security controls (defense) are placed throughout an information technology (IT) system. Its intent is to provide redundancy in the event a security control fails or a vulnerability is exploited that can cover aspects of personnel, procedural, technical and physical security for the duration of the system's life cycle.
- **Dos/DDos:** In computing, a denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.
- **Key logger**: Keystroke logging software is one of the oldest forms of malware, dating back to typewriters. It's still popular and often used as part of larger cyber-attacks.
- **Patch/Patching:** A patch is a set of changes to a computer program or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually being called bug fixes or bug fixes.
- **Whitelisting:** Whitelisting (also referred to as allow-listing) is the practice of explicitly allowing some identified entities access to a particular privilege, service, mobility, access or recognition. It is the opposite of blacklisting.

1. INTRODUCTION

Cyber security is the development, management, and use of information security, OT security, and IT security tools and techniques for achieving regulatory compliance, defending assets, and compromising the assets of adversaries of the organization. On the other hand, Cyber defense is a computer network defense mechanism that includes a response to actions and critical infrastructure protection and information assurance for organizations, government entities, and other possible networks. Nevertheless, Cyberdefense focuses on preventing, detecting, and providing timely responses to attacks or threats so that no infrastructure or information has been tampered with. With the growth in volume and the complexity of cyberattacks, cyber defense is essential for most entities to protect sensitive data and safeguard assets. Cyber defense provides the much-needed assurance to run the processes and activities, free from worries about threats. It helps in enhancing the security strategy utilizations and resources in the most influential fashion. The cyber defense also helps in improving the effectiveness of the security resources and security expenses, especially in critical locations of enterprises (Galinec et al., 2017). Well-defined cyber security and cyber defense plan can improve cyber resilience and business growth.

1.1 Background and Problem Identification

Cybersecurity control is an essential tool for any organization that seeks to protect its customers, employees, and corporate information. Defining the current and future state of a cybersecurity landscape provides clarity and assurance about cybersecurity that senior executives crave. A cyber security plan also enables IT to communicate effectively about how cybersecurity capability is positioned within an organization (Silva et al., 2018).

While enterprises strive to improve information system security by investing in different technologies, the increasing sophistication of information systems attacks has also resulted in the need for joint information-sharing endeavors. A significant difficulty for firms defending against advanced information security attacks is the time gap between the attack and corresponsive response. This can be incredibly long when the firm has no previous knowledge of the kind of attack they face. A proper Cybersecurity defense plan with guidelines, equipment (software, hardware), and skilled resource can resist the potential attack. That is why organizations prepare a strategy based upon current trends, existent threats, IT systems type, resources, and cost, which minimize impact after a breach occurs.

1.2 PROBLEM JUSTIFICATION

Many companies do not seriously prepare IT strategy and plan, especially in cybersecurity, through its importance for further growth of the company. Proper strategy and well-planned IT security systems can save money and not only maintain cyber resilience but also keeping an immense contribution to the development of business and future expansion. For example, medium / large organizations can suffer if they fail to design the dynamic architecture of the network, storage, and software for keeping up IT service alive. As most of the large European companies use versatile software like ERP, CRM, etc., UI design and software & data security could be vital for growth and decision-making. Even unauthorized access can consider a significant security threat. Proper alignment of business processes with information technology systems can hamper operation, productivity, and incise cost. In the bigger picture, it may cost permanent damage to brand reputation, which deteriorates the value and company share.

That is why the impact of a failed Cybersecurity strategy is much higher for any business because it associates with risk, cost, and value. To get protection from future cyber threats, strategies can be developed to fill the gap between current and planned. As all the medium/large enterprise uses IT and services widely for running their business, strategic IT security planning is also considered part of business strategy to achieve bigger objective and excellency with adequately informed decision to invest in Information systems and security.

An Information Technology Strategic Plan (ITSP) aims at discovering the resources and IT in an organization to direct the technological and information architecture to its strategic objectives (Stiawan et al., 2017). The first step to creating an effective IT strategic plan is to start with reviewing the organization's strategic plan, which helps identify the areas where the use of technology can improve operations (Roy, 2016). In recent years, with the improvement of economic sustainability, large companies are encouraged to move to cloud platforms. Despite easy operation and maintenance, there is a considerable risk exist in IT and Information Systems Cybersecurity. After the Covid-19 pandemic crisis, many companies have to reduce costs and migrate the number of applications or systems in cloud platforms to reduce the budget. As the diversity and depth of cyber-attacks have been changing, tech leaders must gear up for next-generation AI-driven cyber-attack on IT infrastructure. When companies start exploring multi-cloud platforms, then security concerns will be severe on multiple platforms. Companies need to think about it and make a strategic plan for protecting their IT systems from future high-tech cyber attackers.

Data protection would be the next challenge for large enterprises. Most of the companies already implemented privacy designs based upon GDPR standards to meet ongoing concerns. Still, in many IT fields, data protection is not working correctly, especially in IoT devices using vulnerable architecture and software components. It will be challenging for organizations not to have a proper plan to deal with such a situation. Many companies use IoT devices and are not still aware of planning importance. My third point would be fulfilling the gap. Companies cannot rely on fresh graduates to meet the required diversity. To achieve a higher level of productivity, companies need to focus on adequate tanning, environment and evaluate the experience.

The next problem is that many companies face making proper decisions regarding transformation. According to Gartner's analysis, about two-thirds of business leaders need to speed up digital transformation to their companies to save grounds from the competitors. In this way, automate business processes can boost productivity. Apart from that, organizations have to face several risks and deal accordingly. Sometimes, they have to prepare for uncertain risks to manage by a proper contingency plan. Moreover, lack of IT funding, IT organizational development, data management, enterprise application integration/upgrades, choosing the right technology or tools for business needs, etc., are the prime aspect that the company's top management and executive body need to focus on planning.

1.3 Research Question

My study is focused on identifying significant issues of Cybersecurity and choosing the right technology for assuring a company’s security and growth. After analyzing scientific paper and CSCD control framework data, I will identify top risky controls that will play a vital role in defining CSCD strategy to defend against cyber-attack. In addition, reviewed CSCD framework will give a constructive guideline for the different levels of enterprises to improve cybersecurity. Research questions are given below:

- What are the strategic elements for Cybersecurity and Cyber Defense control framework?
- How can CSCD risk assessment for inactive control contribute defining CSCD strategy, planning, and maintaining cyber resilience for the enterprises?

1.4 Study Objectives

The research objective is to propose a CSCD strategic control framework and identify top risky controls. In order to reach this goal, the following intermediate objectives are defined:

- Study the current trend of Cyber Risks, Governance, and aspects of new strategical cybersecurity defense planning.
- Study the cybersecurity & cyber defense control Framework.
- Present CSCD Control Framework based on analyzed scientific research papers, previous best practices, and frameworks.
- Present top risky CSCD control and sophistication level diversity based on RMM level.

1.5 Study Relevance and Importance

Cybersecurity is now considered an essential part of individuals to organizations and educational institutions to all kind of financial institutions. Families and parents need to protect their children and family members from online fraud. In terms of financial security, it is crucial to secure our financial information that can affect our personal financial status (Kumar, 2015). Gone are the days of simple firewalls and antivirus software being your sole security measures. Business leaders can no longer leave information security to cybersecurity professionals. GDPR and other laws mean that cybersecurity is no longer something businesses of any size can ignore. Security incidents regularly affect businesses of all sizes and often make the front page causing irreversible reputational damage to the companies involved (Aspa, 2017).

For all of the responses mentioned above require a strategy and planning to protect against threats and cyber-attack. Medium and large enterprises have much concern about security and data confidentiality. Apart from that, the primary cybersecurity threats and trends are Phishing, Ransomware attacks, Cryptojacking, Cyber-Physical Attacks, State-Sponsored Attacks, IoT Attacks, Salami attacks, security vulnerability on Smart Medical Devices and Electronic Medical Records (SEMR), attacks by the third party, attack in a driverless car, social engineering, unauthorized access, etc. After analyzing the number of scientific papers, I realized that there are relatively fewer papers are exsisted to guide multi-level organizations for defining CSCD strategy and planing for maintaining cyber hygiene. Hence, a result of a comprehensive risk assessment to identify inactive controls risk have not been done in other scientific paper. My research drives these enterprises to take a strategic plan based on future cyber-attack and safeguard their information systems. By my research, different types of organizations and sectors like the energy sector, health, IT, research laboratory, financial organization, SME, telecom sector, space technology, etc., will be benefited to create a positive impact in a safe IT or cybersecurity environment.

Moreover, my research will develop some scientific benchmarks and approaches of the cybersecurity control framework for different types of organizations based on their risk management maturity level. In the future, researchers can get direction from my analysis. Nevertheless, top managers or C-level executives (CTO, CIO, CISO, CEO, etc.) can get a compact guideline within a framework control to establish a proper CSCD strategy, planning, control, and governance for the respective enterprise.

2. LITERATURE REVIEW

Nowadays, organizations like banks, telecom, or IT service providers face many cybersecurity threats to carry on their day-to-day business operations. To defend and safeguard IT systems from new cyber-attack, enterprises need a cyber-defense strategy. To prepare the right plan and action in this regard, we must understand the respective IT infrastructure, strategic elements, governance framework of the company. Basically, a cyber-security strategy would be a combination of preventive measures and preemptive action of the security incident or breach. Cyber-security is both a strategy and operational framework, a field of operational capacity, an element of cross-disciplinary and trans-disciplinary approach that is fit to all levels of socio-political, economic, engineering, IT, legal, and security-led levels of theoretical approach and practicability uses and issues (Efthymiopoulos, 2019). For financial and customer-oriented businesses cyber defense strategy would consider as a business defense strategy that mainly relies on cybersecurity and cyber defense policy for maintaining security resilience.

2.1 STRATEGIC ELEMENTS FOR CYBER SECURITY AND CYBER DEFENSE:

To prepare a cybersecurity strategical approach and governance framework, it is crucial to be aware of the strategic elements for cybersecurity and defense. A proper strategy can be made if it covers all the necessary aspects of this domain. To prepare strategic criteria to implement and governance strategies, the elementary understanding needs to clear. In this fast pacing world, the structure, nature, and technology have been changed dramatically. Making all balancing together a combined strategic element view can help choose the right approach for the enterprises.

2.1.1 Variants of Cyber Attack

At first, we need to know the most common variant of cyber-attacks. According to this paper (Stiawan et al., 2017) most common cyber-attacks, including their type and attack process in the following Figure 1: Different variants of Cyber Attacks. Here Trojan and Malware attack through web servers to website. They manipulate the system and get unauthorized access using a virus and hamper the usual activity of the website. Key logger, Dos/DDos, botnet, phishing are the most common approaches to do attack. On the other side, different kinds of Trojan and Malware can attack through mail server users. It appears mainly through an email body, an attachment, or an URL with a virus that can access the user email box even to the entire device. Another type of attack is SQL injection. This is a malicious code injection technique that can access a database and manipulate it. Because of website or Database defect, Database structure fault or improper privilege can increase the chance of this attack.

Apart from that, web phishing, password guessing (Brute Fore, Directory attack, Hybrid attack), Dos are the common and very effective forms of attack. These mentioned techniques can massively attack any organization. It will cost financially for the enterprises, and reputation, trust, and brand value will be demolished.

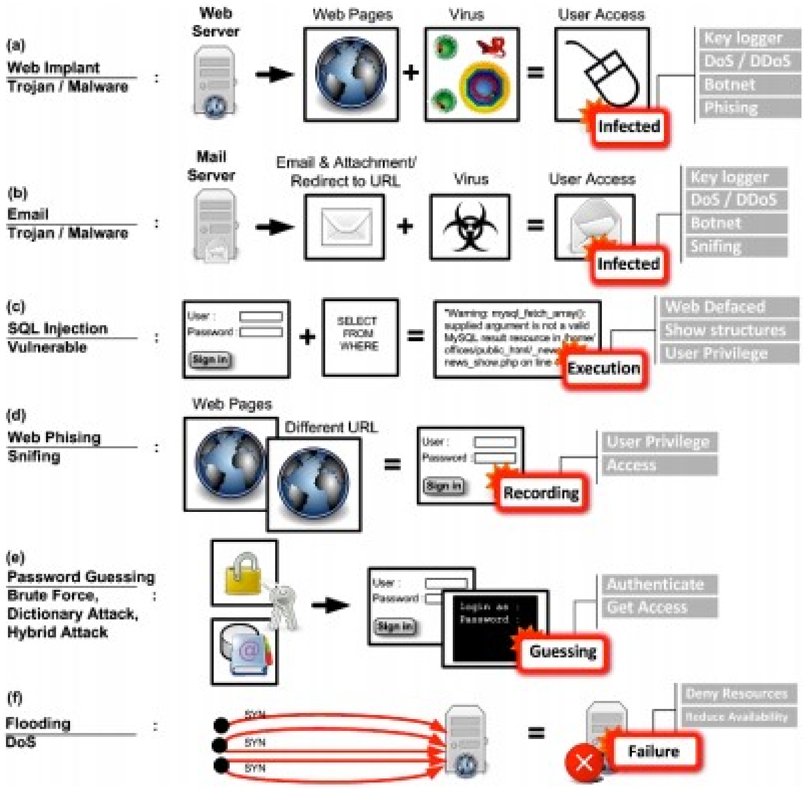


Figure 2: Different variants of Cyber Attacks (Stiawan et al., 2017).

Based upon the targeted nature, hackers attack using mentioned attack mechanism to highly important systems. If an enterprise can identify potential attack criteria, it can identify risk and plan to protect its critical systems. That would be helpful to prioritize the security requirements and investment for a constructive strategical approach.

2.1.2 Recent Cyber Threats

Awareness about the current trend of cyber threats is the critical element for making a strategy. Every year, new types of threats pop up, and most of the time, enterprises do not get adequate time to respond and identify the attack. Some authors sorted out the pattern of new cyber threats that need to be considered for making safeguard policy.

According to Forbes, about 83 percent of enterprise workload will be on the cloud by 2020. Some cloud services increase the threats will be increased gradually, which will be considered Cloud vulnerability. Unauthorized access, control plane attaches, Data breach, Migration module attack, insecure interfaces and APIs, and misconfiguration are among the top cloud security threats needed to consider making cybersecurity strategy (Majhi & Dhal, 2016).

AI-Enhanced Cyber threats are increasing these days. AI and machine learning have enormous capability to attack any kind of system with a high accuracy rate successfully. AI also can be used to safeguard and identify criminals. Apart from that, AI Fuzzing, Machine Learning Poisoning, Smart Contract Hacking, Social Engineering Attacks, Deep fake are the new trends of cyber-attack. (Caldwell et al., 2020).

2.1.3 Business Centric Strategic Elements

An organization needs to know its IT asset first to prepare a cyber-security and Cyber Defense strategy. Then the running service and process need to know as they may be interrupted after a cyber-attack. Here critical can be sorted out according to the sensitivity. Enterprises can identify their systems/services and data according to their business criticality for operational activity. Moreover, having a clear idea and action about Employees, contractors, third parties, and customers can give a broader view to make a proper strategy for them. Knowing the in-depth IT capability is essential. Without adequate infrastructure, software, and skilled IT resources, it would be challenging to assure Cybersecurity. Increase vigilance can improve the chances of stopping the incoming attack. That is why vigilance capability would consider a key for a company. If the Cyber Security and vigilance capability are ensured, it would be much easier for the enterprises to keep resilience in their Cybersecurity (KPMG, 2019).

2.1.4 Cyber Security and Cyber Defense (CSCD) Governance

Cyber Security and Defense Governance are responsibilities and defined practices that direct the control to determine who is authorized to do what activity in terms of Cyber Security and Defensive operation to protect the organization’s assets. Cybersecurity governance refers to the component of enterprise governance that addresses the enterprise’s dependence on cyberspace in the presence of adversaries (Bodeau et al., 2010). Cybersecurity governance thus encompasses information systems security governance; whether information systems security governance can be identified with information security governance depends upon how narrowly or broadly the enterprise construes information security (Arunkumar et al., 2013).

To maintain cybersecurity resilience, there is no other option to strengthen good governance. In this paper (Pernice, 2018), researchers also point out that good cybersecurity governance can prepare organizations to defend against potential cyber-attack. For this reason, a strategy and a suitable model are necessary to prepare according to the nature of the business objective, innovation, vision, and goals. A strong cybersecurity strategy can achieve a competitive advantage by managing risk, facilitating operational excellence, increasing brand reputation, technology/system integrity. To develop an efficient Cybersecurity operating model, Senior or top management of the organization needs to assess current risk, existing assets, strength, managing domain, and capability. Cyber Maturity Assessment (CMA) can provide an illustrative view of the maturity of Cybersecurity and Defense capability. CMA Enables us to understand enterprise management about vulnerability, identify and prioritize areas for remediation and demonstrate corporate and operational compliance that turns information risk into a business advantage (KPMG, 2019).

Most of the IT and cybersecurity-related strategies will be similar in different organizations upon the technology variant. Governing Cybersecurity activity is not kind of the process to do once in a time. It could be a systematic and repetitive process that can be vital for the entire security aspect. People are critical elements to mediate relations and provide support, communication, and technology-related applications and services. Unauthorized and irresponsible human activity can be a threat to a company.

Nevertheless, security should be a concern for each employee in an organization, not only IT professionals and top managers. One effective way to educate employees on the importance of security is a cybersecurity policy that explains each person's responsibilities for protecting IT systems and data. A cybersecurity policy sets the standards of behavior for activities such as the encryption of email attachments and restrictions on the use of social media (McAfee, 2020).

Cyber Security Policy can define the data flow and define legal, operational, and ethical responsibility. Moreover, it can take a vital role to maintain according to other security standards and compliance. In that way, enterprises upgrade IT architecture in a standardized manner according to the policy so that application integration, collaboration, and performance contribute to cybersecurity.

On the other hand, Risk management is another big part of governance. Risk management is the process of identifying potential risks, assessing the impact of those risks, and planning how to respond if the risks become a reality (Wu, 2019). Employes of the organization are the primary asset. They need to be aware of future responsibility according to a governance structure and potential risks to play an active role in the security breach. We can get an idea of how humans can play a vital role in Verizon’s 2018 data breach investigation report. Remarkably they found in their investigation that 93% of all data breaches are caused directly by phishing activity where human interaction is fully involved (Wu, 2019).

To prevent this attack organization's risk culture needs to evaluate. That is why enterprises focus on building a safe cyber interaction culture, train and delegate employees to identify and mitigate risk from various levels. If any incident happens, it would be determined and mitigated within the shortest time. Building separate risk analysis and incident response teams and coordinating all these activity governances can strengthen the organization.

2.1.5 Cyber Security and Defense Intelligence:

To understand the attack type, we need to assess the attack. The research papers of (Hutchins et al., 2011) and (Karen Scarfone et al., 2008) studied cyber-attack assessment and defense. They also referred to a model called cyber kill chan. This model gives an idea to a defender to develop resilient mitigations against intruders and intelligently prioritize investments in new technology or processes and drive defensive courses of action.

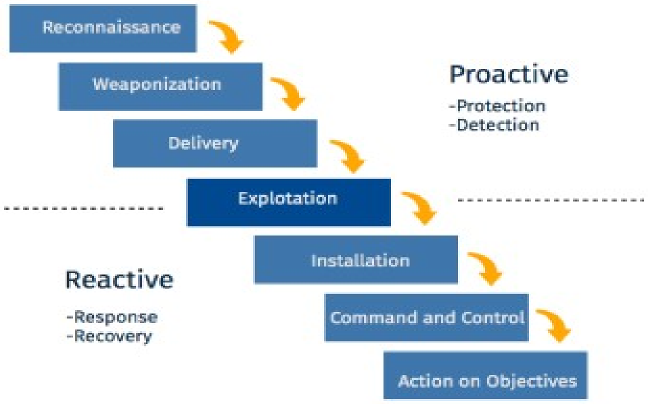


Figure 3: Kill chain model for cybersecurity and defense (Hutchins et al., 2011)

The author represented this kill chain model specifically for cybersecurity intrusions. This model is build considering computer network attack (CNA) or computer network espionage (CNE). Here in the model, reconnaissance is defined for research, identification, and selection of the target. The author wanted to describe the automated tool without the proper authorization to the system like Trojan by weaponization. The next step is the transmission of this weapon to the targeted system. Usually, by email, USB, attachment, file, or another medium, it can weaponize this. After entering successfully, exploration can trigger according to the plan by a hacker to the victim host. On that occasion, most of the time, victims cannot understand what is happening to their system. After that, Trojan can install a virus program so that they can persistently stay in the victim system and operate unethically. The victim system fully gets controlled by the hackers in this stage of C2 (Command and Control). They do not need to present to operate the system physically. All the access and command control mechanisms compromise by hackers. In most cases, the principal intention is to data exfiltration, encrypt, or blockage access from sensitive files or systems from the target systems.

Here in the cybersecurity and defense kill chain, priorities analysis, detection, and synthesis are divided into proactive and reactive activity. The authors also mentioned adequate protection and detection measure could be taken in the visionary phase. Reconnaissance, Weaponization, Delivery, Exploration are the steps considered as a proactive activities. On the other hand, from exploitation, installation, C2 (Command and Control), and Action on the objective is regarded as a Reactive stage that means it required Response and Recovery.

On the other side, researchers from this paper (Röcher, 2018) considered this kill chain model a cyber-attack methodology. They also agreed that a solid cybersecurity intelligence could stop the progression of the attack from preliminary steps, and organizations can take time to respond accordingly to safeguard their IT systems and data.

2.1.6 Strategic Cyber threat intelligence (CTI) :

In these recent years, enterprises improve their Cyber threat intelligence (CTI) competency using adequate technology, structured processes, well-trained people. This whole system can be responsible for gathering intelligence to enhance security. Such capability will ensure quick identification of any threat to detect it precisely and make proper response quickly. This CTI approach can play a vital role in cyber defense. Enterprise can easily be aware of new threats by external and internal intelligence. Here external intelligence means gathering and analyzes data regarding the pattern, sources, target, intention, losses, attacked system technology, response activity, etc., of cyber-attack in a similar industry. Exchanging data and ordinary intelligence among similar industries of central cybersecurity agencies from the government can also play a significant role in CTI. Nowadays, companies put more focus on internal intelligence to safeguard from cyber-attack. For this reason, all kinds of access monitoring, central alert system implementation, monitor suspicious activity.

A well efficient Cyber threat intelligence center (CTI) can carry significant importance for a company. By proper analysis and surveillance, it can reduce potential cyber risks. Furthermore, data leak prevention is a prime objective these days. Through accurate monitoring, CTI can identify the loophole of data bridge and possible difficulties if IT or business operation reduces risks. On the other hand, despite being attacked, CTI can reduce costs in many ways. For example, post-incident investigation, figure out loss, suspect identification, fine calculation, lawsuit charges can be reduced if a proper CTI center works efficiently.

Moreover, CTI can empower organizations by focusing on critical systems with all relevant security aspects to take less time to respond to any cyber-attack. CTI also has a few more importance on the strategic element. CTI can analyze the new state of the earth technique by cybercriminals. That way, an organization can get time to research a new approach to defense. Sometimes they can change the architecture or upgrade technology to protect themselves, which would play a vital role in the cybersecurity and defense strategical approach. Even they can find a way around to block the attack. Another crucial thing that CTI can play for a whole industry sector with sharing intelligence. In recent years many countries trying to follow this approach, specially EEU and North American countries, to safeguard from attack and make a dynamic strategic approach (Mavroeidis & Bromander, 2017).

2.2 CYBER DEFENSE MODEL STRATEGIC APPROACH:

Cyber Defense is one of the crucial parts to mitigate or respond to a cyber-attack. It also assists the users to link and transit between dimensions and sub-categories to apply appropriate defense mechanisms to cope with the ever-changing nature of cyber-attacks. Using an appropriate defense strategy requires the identification of all the key actors in cyberspace (Kolini & Janczewski, 2015).

After researching the number of scientific papers on Cyber Defense, a model was proposed with a taxonomy divided into three distinct dimensions. For a constructive Cyberdefense strategy, it is crucial to identify a thorough process in deep. To prepare a Cyberdefense strategy, an organization needs to understand the defense element and the capabilities to do. In that way, it would be easy to make an appropriate strategic approach for the respective company. Without a proper understanding of the cyber defense model, it would be challenging to decide.

In that way, to represent a well efficient cyber defense base model, other authors described a high-level approach but, this author emphasizes OODA loops for the cyber defense model (Zager & Zager, 2018). Researchers have combined the OODA loop with the NSA Methodology for Adversary Obstruction to create a new cyber-defense model. The concepts of the OODA loop are used to make cybersecurity trustworthiness assessments (Arunkumar et al., 2013). OODA loop also allows you to learn from your past experiences and loop it again. That gives the improved performance after finishing and starting the loop.

On the other hand, if we compare this model with the author tried to represent a cyber-defense model based upon the capability with asset and preparatory process (Kolini & Janczewski, 2015). In an IT environment, assets are company-owned information, software, and hardware used in business activities. In this paper, People are also considered because of having skills to react and prevent something. Even they are also the facilitator for any IT services. On the other hand, the preparation process is the readiness to protect from cyberattacks which will help to prepare a solid cyber response plan. For a cyber-defense strategy, the importance of such a preparation process is indispensable. Researchers included planning, communication, activation, and evaluate this process.

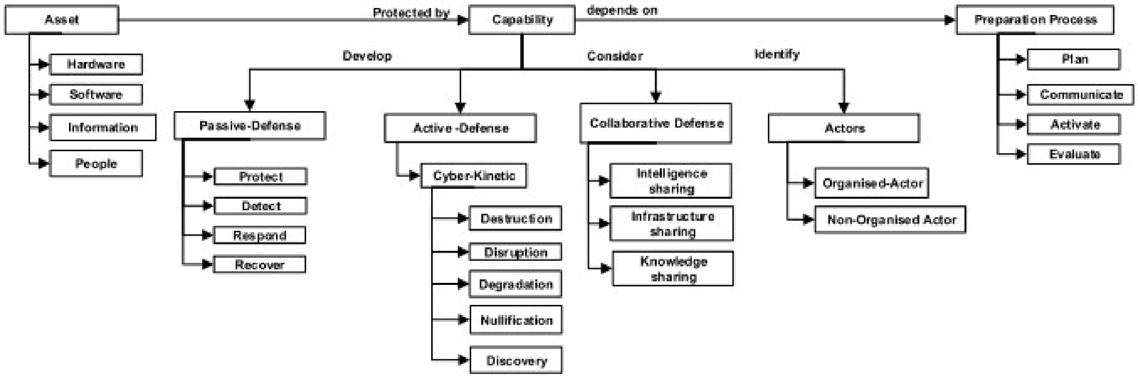


Figure 4: Cyber capability defense model (Kolini & Janczewski, 2015).

As the author prepared this model based on capability, they segregated defense in different stages. The first capability they mentioned is Passive Defense. Keeping cyber resilience with the protection of IT assets from cyber-attack, this part is highly dependent though it mentions as a passive defense role. Passive defense includes Protect (Whitelisting, Defense-in-depth, patching), Detect (monitoring, Surveillance, Interception), Respond (Network Segregation, Sill Switch), Recover (Disaster Recovery, Business continuity). Here protect and Detect can be considered a pre-attack stage, and Respond and Recover considered attack failure can cause serious harm to the company.

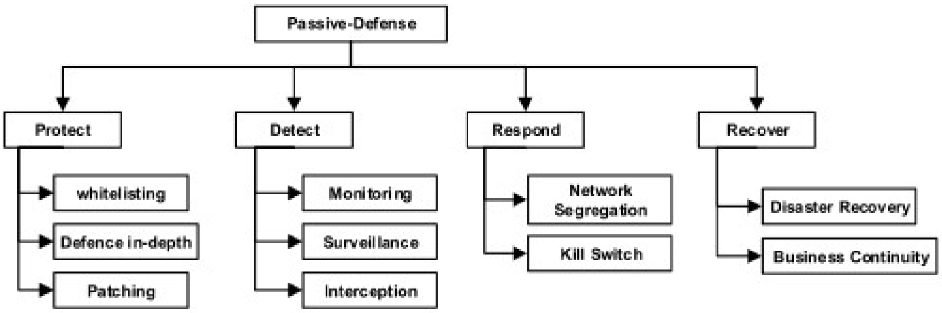


Figure 5: Cyber capability passive defense model (Kolini & Janczewski, 2015)

The following capability of Cyber Defense is Active Defense. It is considered a direct war with attackers. Even a researcher from this paper (Rosenzweig, 2013) *refers* to active defense as a real-time capability to minimize the impact of cyber-attacks. The author made Cyber Kinetic a branch of Active Defense divided into Destruction, Disruption, Delegation, Nullification, and Discovery. According to the knowledge from the related paper, it is pretty much understandable that Active defense capability would increase upon technological improvement, standardization of systems, and well-trained IT resources. In recent years, social engineering, also considered part of discovery, can gather data about human behavior.

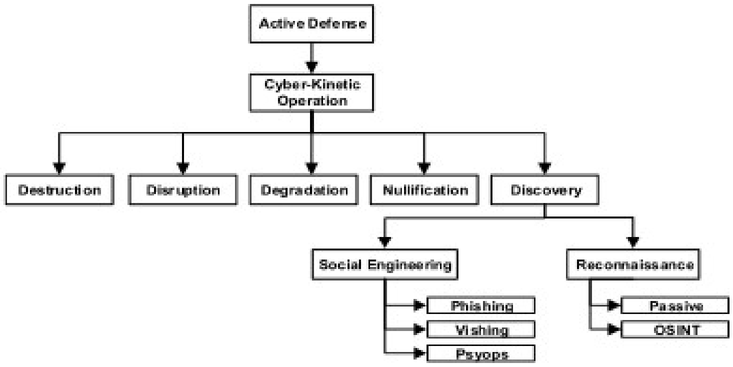


Figure 6: Cyber capability active defense model (Kolini & Janczewski, 2015)

The following figure (Figure 3.2.4: Cyber capability collaborative defense model) illustrates the collaborative defense, which includes intelligence sharing, knowledge sharing, infrastructure sharing.

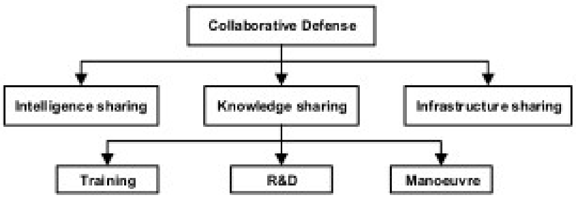


Figure 7: Cyber capability collaborative defense model (Kolini & Janczewski, 2015)

In this paper, researchers provided many clear elements of Actors. They wanted to illustrate the major actors of Cyberdefense so that it would be much understandable to whom we need to collaborate and cooperate. Organized actors give a high-level structural idea about the cyber defense that needs liaison with international authorities. Besides, authors represent Non Organized actors too. Hackers, Hacktivists, Whistleblowers, cyber warriors are part of the not organized actors.

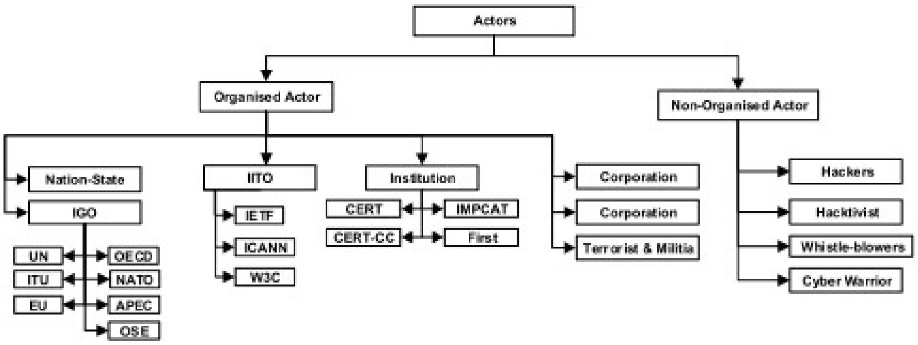


Figure 8: Cyber capability defense actors (Kolini & Janczewski, 2015)

This cyber defense model gives a deeper understanding of the capabilities of an organization. It would be much identical and accessible to any modification and emphasize where it is needed for building a strategy. The component they mentioned is playing a vital role in the landscape of cyber defense strategy. In this world, the capability of swift response means a company is prepared to do in defense at any time. In fact, a solid Cyber Security and Defense strategic approach impacts the overall efficiency of the whole organization more in a positive manner.

2.3 Cyber Security Strategic Pillars:

For developing a strategy, there is a number of pillars. One researcher demonstrates the fundamental pillars of effective international standard cybersecurity strategy, which is proposed based on (ISO/IEC, 2013). The organizational characteristic of cybersecurity is a set of recommendations from the simple person to the whole world. In this first pillar, we treat two concepts: Policy and Formation (Elkhannoubi, 2015). Here, the policy is applied all over the organization to enforce a new set of rules to standardize and efficient processes. Also, it can be used internally of the organization and externally of the organization among different departments of the specific spectrum of it. The rest of the two pillars they mentioned are Legal and technological. All respective contractual legislation, fulfilling cyber law, and regulatory compliance are considered under the legal pillar. Here technology is used as a reference ground to provide best-practice guidance for IT service management. With reference to upon paper, researchers illustrated the importance of the technology pillar. It service or data availability management, IT service continuity management, IT security management, Incident management are the core part of the Technology pillar. It is pretty clear that without technological improvement, any kind of cybersecurity strategy will not work out properly. That is why cybersecurity strategy should always be progressive upon new technological innovation, use, and technology adoption properly. If an organization cannot cope with new technology, business continuity and cyber defense will be seriously hampered. Even it would difficult to service compete with other company in the same industry.

Besides, another researcher presented how human behavior can play a vital role and be considered a cybersecurity defense strategy. “Many ignored the context in which much cybersecurity behavior occurs (i.e., the workplace), and the constraints and other demands on people’s time and resources that it causes. At the same time, there was evidence that models that stressed ways to enable appropriate cybersecurity behavior were more effective and useful than those that sought to use threat awareness or punishment to urge users towards more secure behavior”(Evans et al., 2016). Moreover, ENISA researchers conducted a CURRENT CYBERSECURITY HUMAN FACTOR STATISTICS survey where the importance of human behaviors in cybersecurity and defense is mentioned. Then, the authors came up with the proposal of a cybersecurity human vulnerability assessment framework (Evans et al., 2016). People can sometimes get tired of security procedures and processes, especially if they perceive security as an obstacle, preventing them from their primary task (e.g., being blocked from visiting a music download website because the browser has stated that the site might have malware). It can also be stressful to remain at a high level of vigilance and security awareness. These feelings describe the so-called ‘security fatigue, and they can be hazardous to an organization or society (Spiller, 2020).

On the other hand, researchers more clearly describe and provide evidence of the Role of Human Factors/Ergonomics in the Science of Security, especially in Decision Making and Action Selection in Cyberspace (Proctor & Chen, 2015). The more considerable danger to our digital space is the threat of unauthorized access. Hackers always try to attempt to get data that is private or used but a set of people. Their one mistake can cause severe damage to a company. This evidence fill with the fundamental knowledge and the idea that people can play a vital role in Cybersecurity and Defense.

3. CONCEPTUAL RESEARCH MODEL

Based on the conducted literature review, a conceptual model is was developed. The main idea of the research will be to propowition a CSCD framework and the identification of top risky control family. Here top risky control means a set of control contains high risk if they are not implemented in the enterprise. To achieve this objective, a clear picture of the CSCD Strategic Element needs to be established at first. Over the time the variation of cyber-attacks has been changing along with the Cyber threats. In order to propose CSCD Framework, it is essential to gather the attack process about current threats. Knowledge about different CSCD frameworks and strategic approaches can be collected from analyzing other scientific papers.

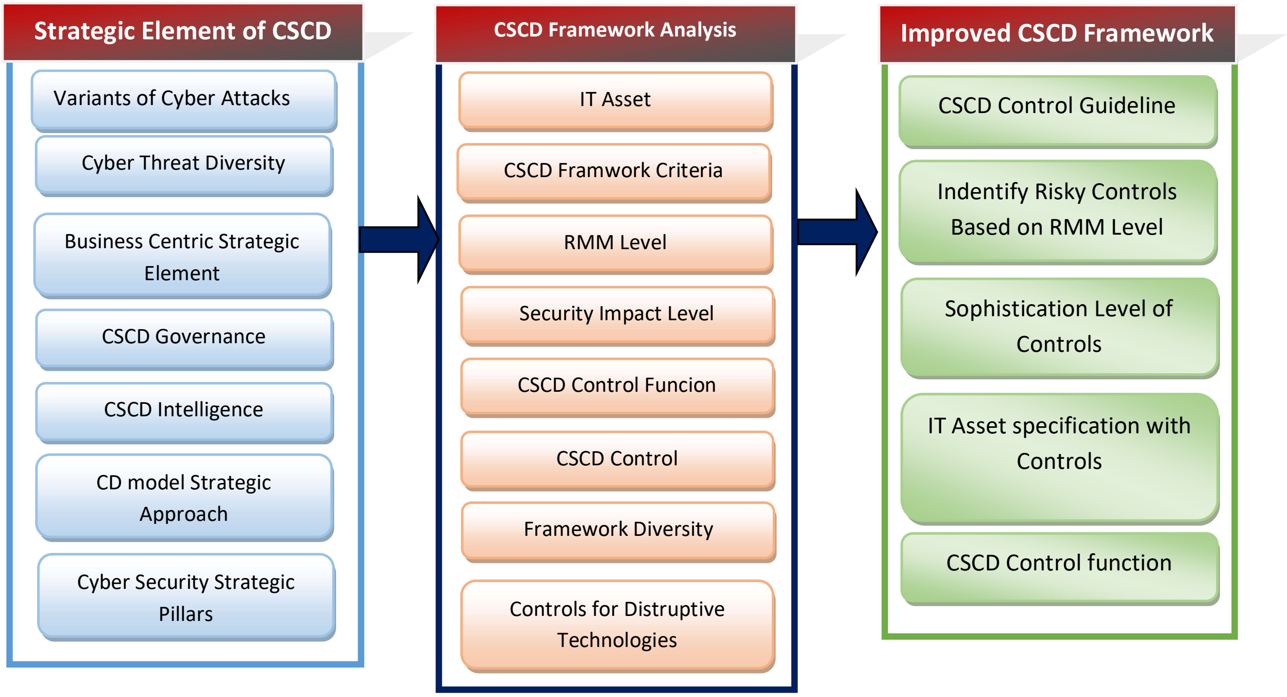

Strategic Element of CSCD
Variants of Cyber Attacks
Cyber Threat Diversity
Business Centric Strategic Element
CSCD Governance
CSCD Intelligence
CD model Strategic Approach
Cyber Security Strategic Pillars
CSCD Framework Analysis
IT Asset
CSCD Framwork Criteria
RMM Level
Security Impact Level
CSCD Control Funcion
CSCD Control
Framework Diversity
Controls for Distruptive Technologies
Improved CSCD Framework
CSCD Control Guideline
Indentify Risky Controls Based on RMM Level
Sophistication Level of Controls
IT Asset specification with Controls
CSCD Control function

Table 1: Conceptual model of research

Document analysis is a form of qualitative research that uses a systematic procedure to analyze documentary evidence and answer specific research questions (Frey, 2018). Similar to other methods of analysis in qualitative research, document analysis requires repeated review, examination, and interpretation of the data in order to gain meaning and empirical knowledge of the construct being studied (Frey, 2018). Some authors published cybersecurity frameworks but proposed an improved version of the framework and some points need to be considered. Proper concept and clear understanding are the keys to this research. Having an appropriate concept of Business Centric Element, CSCD governance, CSCD intelligence, and Cybersecurity strategic pillars will be considered the main backbone to start developing the CSCD framework because the proposed research requires thorough investigation and understanding of each strategic element. It is highly important to analyze the framework. Without analyzing the existing framework, it will not be possible to get a clear understanding of framework criteria and CSCD strategy. Based upon the strategic part, the component of the CSCD framework component is defined for an improved version.

As the proposed framework is to be developed based on some renowned frameworks and guidelines, some improvement criteria need to be identified and integrate with the proposed framework development, improving control quality and providing a more transparent view to implement in the enterprises. During CSCD framework development, identifying the core element from the different diverse frameworks and adapting to the new guideline will make the framework more implementation friendly. Apart from that, we have seen the use of disrupted technologies is getting high in different enterprises. Most of the time, cybersecurity control is not much well defined for such technologies. This research will analyze the existing defined cybersecurity guidelines for disrupted technologies from different scientific papers. Cybersecurity control will be selected according to CSCD control type and criteria. Each element of CSCD framework development is vital to propose an improved version of the framework.

The improved CSCD framework will include control guidelines according to security impact, organizational risk management maturity, and sophistication level. Moreover, each control is defined by control functions. New control guidelines mapped with criteria are considered as the improvement. The proposed framework will be designed with a number of new criteria. Each criterion defines the different aspects of the specific guideline. The priority, implementation pathway and categorization gives a clear idea about each control with regards of Cybersecurity and cyber defense aspect. Top risk controls have been identified throughout the holistic risk assessment score. Throughout the risk assessment, the risk impact of the emterprises for inactive controls can be identified.. A list of risky control according to different RMM levels is the outcome from the analysis and preparing control framework. Based on that, the enterprises can define a more accurate strategy for ensuring security resilience.

4. RESEARCH METHODOLOGY:

To design overall work, exploratory type research design is followed throughout the research. This research typically involves qualitative methods to maintain quality, segregating category and better representation. Data analysis and model of CSCD control framework have been prepared to be based on Secondary data analysis and framework observation method of qualitative research.

At first, I studied and analyzed the current CSCD Planning, Governance, and Control Guideline issue from different scientific papers was studied and analized to gather ideas, concepts, best practices, and a holistic view of the research objective. Document analysis is a form of qualitative research in which documents are interpreted by the researcher to give voice and meaning around an assessment topic (Bowen, 2009). During the analyzing stage, many scientific papers and leading frameworks provide ideas about framework structure. Different approaches and diversity of frameworks are identified, and observations are noted for the work and control baseline preparation.

Throughout this process, criteria of control baseline are developed. In a broad way, a comparison of different scientific papers, frameworks, and sources will be analyzed and mapped at one point to prepare the CSCD control framework. In this way, it enables the analyst to specify which elements of a framework are particularly relevant to particular questions and to make general working assumptions about the shape and strength of these elements where theories make assumptions that are necessary for an analyst to diagnose a specific phenomenon, explain its processes, and predict outcomes (Ostrom, 2011). Both data collection and analysis part is carried out by the qualitative research method. Different frameworks, theories, security models need to be analyzed carefully. The main objective is to prepare an improved CSCD framework with control guidelines and identify risky top control. The accuracy of the CSCD framework development depends on the research paper and the existing frameworks analysis part. Based upon the literature review, some parts are identified to improve. Precisely, CSCD impact criteria, organizational risk management maturity (RMM) level, and sophistication level of controls are recognized throughout the literature review for the improvement. Apart from that, the framework diversity and other guideline identification will be carried out in the development phase. The proposed hypothesis will be carefully evaluated and integrate with new framework development. This process will be followed by the quantitive research method. A theoretical model will be developed for setting the criteria based upon the concept, models, and secondary data from previous research papers. Besides, the new additional control guideline will be followed according to general qualitative inquiry. This approach will provide greater flexibility to collect information from the different frameworks and scientific papers.

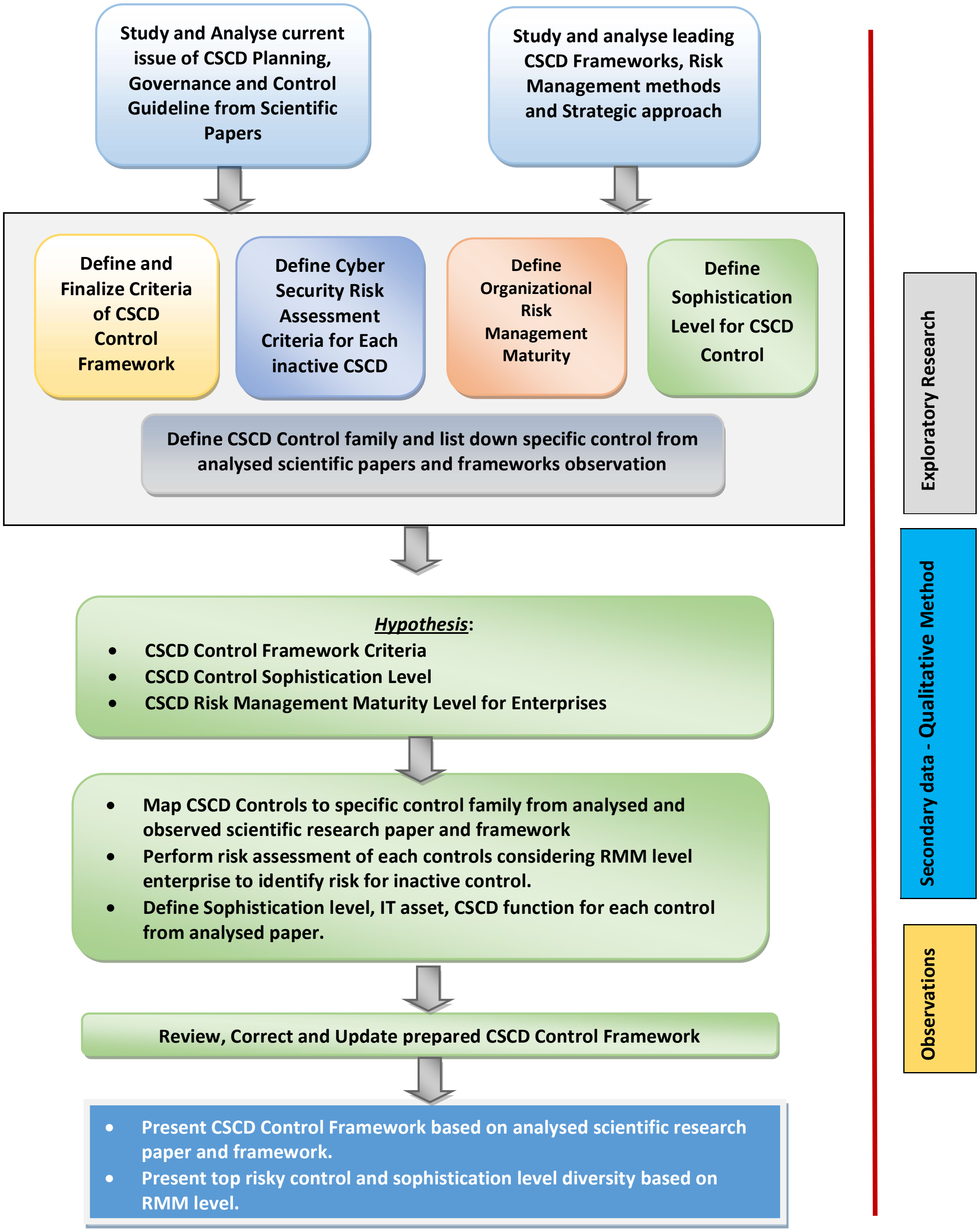

Study and Analyse current issue of CSCD Planning, Governance and Control Guideline from Scientific Papers
Study and analyse leading CSCD Frameworks, Risk Management methods and Strategic approach
Define and Finalize Criteria of CSCD Control Framework
Define Cyber Security Risk Assessment Criteria for Each inactive CSCD
Define Organizational Risk Management Maturity
Define Sophistication Level for CSCD Control
Define CSCD Control family and list down specific control from analysed scientific papers and frameworks observation
Hypothesis:
CSCD Control Framework Criteria
CSCD Control Sophistication Level
CSCD Risk Management Maturity Level for Enterprises
Map CSCD Controls to specific control family from analysed and observed scientific research paper and framework
Perform risk assessment of each controls considering RMM level enterprise to identify risk for inactive control.
Define Sophistication level, IT asset, CSCD function for each control from analysed paper.
Review, Correct and Update prepared CSCD Control Framework
Present CSCD Control Framework based on analysed scientific research paper and framework.
Present top risky control and sophistication level diversity based on RMM level.
Exploratory Research
Secondary data - Qualitative Method
Observations

Figure 9: Research Methodology Overview.

After this step, the defined hypothesis will be integrated into the proposed framework. To do that, the main activity will be the mapping of the existing control guideline upon the specified criteria.

Here, pointing IT asset, control sophistication level, organizational maturity grade, CSCD control functions are the set of criteria where the controls will be assessed and defined. Nevertheless, mapping and adding new control in the guideline framework requires extensive review and analysis of the scope of work. The source of reference was maintained appropriately in each control during the data analysis part. Based on the related model and best practice, the whole control guideline review will be conducted in the qualitative method of the research model. This method is an approach that revolves collecting, analyzing and mixing quantitative data in a single study or series of studies in the belief that the information will provide a better understanding of the phenomenon than the methods would do separately (Schram, 2014). In that way, the proposed CSCD control guideline will be defined. Microsoft excel has been used as the data repository to make the CSCD control baseline and assessesment of the risk of each control. Also, Microsoft Excel-based data modeling and analysis is used in the research.

5. CSCD CONTROL FRAMEWORK FOR STRATEGIC GUIDELINE AND PLANNING

5.1 Assumption

Based on a study in the literature review, about cybersecurity, cyber defense, Cyber Risk, Vulnerability, Cyber Hygiene, Cybersecurity and defense strategy, etc. I have understood that the researcher has to be more focused, careful, and knowledgeable in many fields. Despite all these, the following requirement must be fulfilled before conducting research activity.

- Having a clear concept of different domains of IT and Cybersecurity is essential. A sound experienced person can not only understand the flow of data but also have clear visibility on the architecture of the systems. For the novice person, it will be a cognitive challenge to get a clear idea of how different IT functionally works and is connected to complete the operational activity. Higher proficiency in information security also suggests better performance in cyber detection than lower levels of knowledge (Bodeau et al., 2010). The researcher required strong expertise in IT hardware, software, network, database, application development, software testing, disruptive technologies, risk, vulnerability, IT strategy, IT management, etc., to understand and analyze.
- Fundamental knowledge about the diverse types of attacks in cyberspace is highly required. The way of cyber-attacks has been changed in the recent years. Attackers are not using the same old techniques as before. Due to the evolving technologies, threat and attack patterns have been adjusted accordingly. These days AI Fuzzing, Machine Learning Poisoning, Deep fake, etc., are the new trending attack variant. (Caldwell et al., 2020). It would be challenging to determine specific attaches' detection and cyber defense mechanism without knowing the attack type.
- One of the most essential things is understanding the difference between the cyber security framework and including controls in the data analysis. Many cybersecurity frameworks are existing, but all are not suitable to consider in the analysis part. Cybersecurity frameworks defending against cyber-attacks have appeared to be generally fragmented and varying widely in effectiveness (Atoum et al., 2014). Moreover, Cybersecurity frameworks integrate a set of high-level conceptual security controls, solutions, entities, tools, techniques, or mechanisms to collectively collaborate Cybersecurity strategy (Atoum et al., 2014).
- Well-defined Cybersecurity and Cyber Defense framework lays out the ground for a conceptual, coherent, systematic, overarching, and consolidated approach to implement cybersecurity strategies (Atoum et al., 2014). Having an understanding of strategy precisely IT strategy, and IT management are the key to this research. Based on CSCD control analysis, a set of data will be produced. Proper illustration of results will help management to define strategies for the organization and implement the guidelines to defend from cyber-attacks.

- Risk analysis is an important activity that organizations must perform to prevent the attacks and/or adverse consequences that can arise from them (Atoum et al., 2014). People using many applications and devices without having much knowledge of them, which increases the risk of cyber threats. Cyberattacks represent an essential issue for all organizations concerned with economic impacts and interested in protecting its full scope of digital. (Henriques de Gusmão et al., 2018) That's is why risk analysis plays an indispensable role in cybersecurity and cyber defense. According to (Patel et al., 2008), risk-assessment methods can be either qualitative or quantitative. Qualitative risk-assessment methods are used primarily in cases where risk-assessment calculations are simple and, therefore, when it is either unnecessary or impossible to quantify threat frequency and other technical issues. The quantitative risk analysis methods are mathematical instruments for evaluating risk where mathematical procedures, such as fuzzy theory, fault trees, and multi-criteria methods, are used. Thus it is pretty much clear that organizations must have complete skill resources who can do risk analysis using the proper technique.
- Data collection is another crucial part of the research. Quality of study will not achieve if data collection is done from an unauthentic source. As this research will be done based on cybersecurity frameworks, choosing an appropriate framework and ability to sort out control will provide many accurate study results. Nevertheless, collecting data from renowned frameworks increases the quality of research and is more effective in improving the control framework from the existing one.

5.2 Study and analyze major Cybersecurity and Cyber Defense Framework and scientific research papers

First, it needs to understand different frameworks for preparing CSCD control and then identifying high-risk control families. Following frameworks are analyzed to do this research.

SL	Framework Name and Reference	Year	SL	Framework Name and Reference	Year
1	NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations (Commerce & Wilbur L. Ross, Jr., 2020).	2020	2	GDPR (General Data Protection Regulation) (Brodin, 2019), (GDPR EU, 2018).	2017
3	NIST Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments (Rebecca M. Blank. Patrick D. Gallagher, 2012)	2012	4	FISMA (Federal Information Systems Management Act) (FISMA, 2020)	2020
5	NIST Special Publication 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems (Swanson et al., 2010).	2020	6	CISA Review Manual (CISA, 2014)	2014
7	NIST Special Publication 800-39, Managing Information Security Risk Organization,	2011	8	Cloud Security Alliance's Security Guidance for Critical Areas of Focus in	2017

	Mission, and Information System View (NIST, 2011).			Cloud Computing v4.0 (CSA, 2017)	
9	NIST Special Publication 800-95, Guide to Secure Web Service (Winograd et al., 2007).	2007	10	CSA, Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure (CSA, 2019)	2019
11	NIST Framework for Improving Critical Infrastructure Cyber security (Barrett, 2018).	2018	12	CSA's Perspective on Cloud Risk Management (CSA, 2020)	2020
13	NISTIR 8183, Revision 1, Cybersecurity Framework Version 1.1 Manufacturing Profile (Stouffer et al., 2020).	2020	14	CSA Guide to the IoT Security Controls Framework Version 2 (CSA, 2021)	2021
15	NIST Special Publication 800-12,Revision 1, An Introduction to Information Security (Nieles & Dempsey, 2017).	2020	16	CYBER RESILIENCE REVIEW (CRR) (Agency, 2020b), (Agency, 2020a)	2020
17	Payment Card Industry Data Security Standard (PCIDSS), Requirements and Security Assessment Procedures, Version 3.2.1 (PCIDSS, 2018).	2018	18	Digital Container Shipping Association, DCSA Implementation Guide for Cyber Security on Vessels v1.0 (DCSA, 2020)	2020
19	ISO/IEC 27001:2013, INFORMATION SECURITY MANAGEMENT (ISO, 2013)	2013	20	ENISA, technical guidelines for the implementation of minimum security measures for DSPs (ENISA, 2016b)	2016
21	ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls (ISO/IEC, 2013)	2013	22	ENISA, Cyber Insurance: Recent Advances, Good Practices and Challenges (ENISA, 2006)	2016
23	IASME Governance standard (Dresner et al., 2018).		24	Cyber Security for Consumer Internet of Things: Baseline Requirements, ETSI TS 103 645 V2.1.2 (ETSI, 2020)	2020
25	SOC 2® - SOC for Service Organizations: Trust Services Criteria (ASEC, 2020)	2017	26	Guideline on Effectively Managing Security Service in the Cloud (Chen, 2018)	2018
27	CIS Controls, v7.1 (CIS, 2019).	2019	28	ISO/IEC Information technology — IT asset management, Third edition (ISO, 1987)	2017
29	CIS RAM (CIS, 2018).	2019	30	ENISA, Cyber Security Culture in organisations(ENISA, 2017)	2017
31	COBIT Framework Introduction Methodology (Lanter, 2019).	2019	32	ETSI TR 103 305 critical Security controls for effective cyber defence (ETSI, 2015b).	2015
33	COSO (Committee of Sponsoring Organizations)(Galligan & Rau, 2015).	2015	34	ENISA, Economics of vulnerability disclosure (ENISA, 2018b)	2018
35	TC CYBER (Technical Committee on Cyber Security) (ETSI, 2015a, 2018b), (ETSI, 2018b), (ETSI, 2016c), (ETSI, 2016b), (ETSI, 2016a), (ETSI, 2018a), (ETSI, 2018c)	2018-2020	36	ENISA, Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity (ENISA, 2018a)	2018
37	HITRUST (Health Information Trust Alliance)(Hitrust CSF, 2020)	2020	38	Fed RAMP (Federal Risk and Authorization Management Program) (FEDRAMP, 2020), (FEDRAMP, 2017a), (FEDRAMP, 2017b), (FEDRAMP, 2018), (Fedramp, 2018).	2017
39	CISQ (Consortium for IT Software Quality)		40	HIPAA (Health Insurance Portability and Accountability Act) (Hipaa, 2020)	2018
41	The Ten Steps to Cybersecurity	2021	42	NIST Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information	2015

				Systems and Organizations (Boyens et al., 2015).	
43	ENISA Work programme: Including multiannual planning (ENISA, 2016a)	2016	44	Bigdata : security and Privacy handbook by CSA (CSA, 2016).	2016

Table 2: Analized major framework and research papers

5.3 CSCD Control Framework Concept

Framework is needed to implement cybersecurity in the national and international environments that address the hyper-connectivity (Dawson, 2017). In this twenty-first century, the use of devices and information systems has been increased than any other time before. For that reason, cybersecurity threats have been improved dramatically, especially on critical information systems and cyberspace. A solid structure and methodology are required to protect critical assets. CSCD framework is a kind of guidelines and best practices that will help identify potential risk on critical infrastructure or asset and direct to mitigate. Literally, the framework is required to straighten the resilience of information systems and safe use of cyberspace (Barrett, 2018). Here the term critical infrastructure is significant for understanding framework structure.

The proposed cybersecurity framework is based on the critical asset. Identifying critical assets for any kind of company is essential. This fast-changing world of information and communication technologies (ICT) and the increasing use of Operational Technology (OT) introduces new cybersecurity-related risks to critical infrastructures (CI), critical information infrastructures (CII), essential services, and societies at large (Ritchey, 2019). In an attempt to mitigate and manage this cyber risk, nations have created or are creating CI protection (CIP) and cybersecurity-related laws and regulations (Ritchey, 2019).

Critical Infrastructure (CI) is defined as “an asset, system or part thereof located in the Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions” (The Council of the European Union, 2013). Apart from that, according to an executive order by ex-American precedent, critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (Obama, 2013) as all type of data is stored in the asset like database, hardware or another electronic device for organization’s business and operation purpose. For this reason, identification of critical infrastructure and asset can make easy to prepare CSCD framework and its implication. Moreover, to manage cybersecurity risks, a clear understanding of the organization's business drivers and security considerations specific to its use of technology is required. Because each organization's risks, priorities, and systems are unique, the tools and methods used to achieve the outcomes described by the Framework will vary (Barrett, 2018).

The National Institute of Standards and Technology's Cyber Security Framework organizes cybersecurity activities in five categories: Identify, Protect, Detect, Respond, and Recover. The recovery category differentiates this framework from all other frameworks. The NIST framework recognizes the importance of recovery planning and suggests the development, implementation, and maintenance of plans for timely recovering and restoring any capabilities or services impaired by a cyber-attack (Roure et al., 2019).

5.4 CSCD Control Framework Fundamental

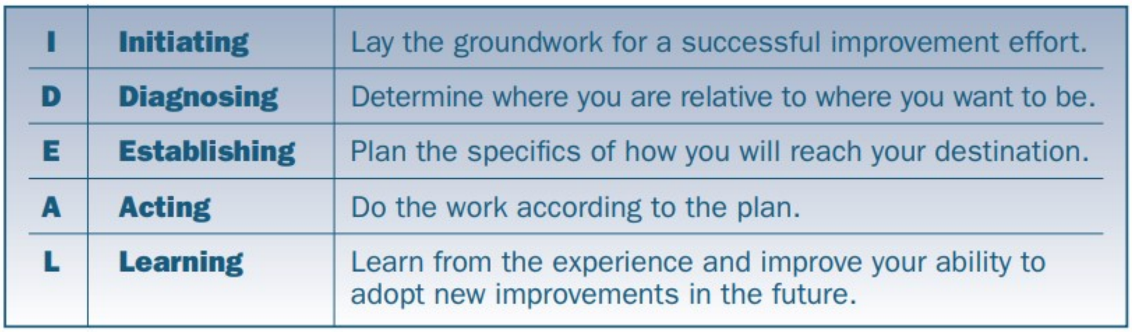
In this part, we will elaborate on some fundamental topics about the CSCD control framework. It is always vital for enterprises to select specific controls that align with their business strategy, functions, priorities, and capability to minimize risk from potential threats. In preparation for selecting and tailoring the appropriate security control baselines for organizational systems and their respective environments of operation, organizations first determine the criticality and sensitivity of the information to be processed, stored, or transmitted by those systems where the process of determining information criticality and sensitivity is known as security categorization (Commerce & Wilbur L. Ross, Jr., 2020). Here its is observed that the author also elaborates the tailoring approach of control baseline on a variety of factors not limited to threat information, mission or business requirements, types of systems, sector-specific requirements, specific technologies, operating environments, organizational assumptions and constraints, individuals' privacy interests, laws, executive orders, regulations, policies, directives, Standards, or industry best practices, etc. In this framework, we collected different controls from various frameworks considering the above tailoring approach for other organizations. Through our research output, we can present a control category based on organizational Risk Management Maturity level (RMM). Different types of organizations are distinguished and categorized based on CSCD control implementation and Cyber resilience maturity level. Since the value of impact may not be the same for a particular system or control for different RMM level organizations, we use score-based impact and likelihood calculation for measuring potential risk for specific controls. Besides, every control has a specific sophistication level based on the defined criteria. This sophistication level gives the understanding of the criticality and perfection of making a CSCD plan and implementation accuracy.

Moreover, CSCD framework function is defined too for each control according to the National Institute of Standards and Technology's Cyber Security Framework, where cybersecurity activates are defined in five categories: Identify, Protect, Detect, Respond, and Recover (Roure et al., 2019). In this framework model, I have underlined subcategories under these CSCD activities. A set of subcategories are listed in a central control category with a similar set of controls based on specific systems/ domains/ technologies. Thus, we can get an idea about CSCD top rules for different RMM level enterprises throughout this research, which will provide a guideline to decision-makers of the organization to make strategies and plan for cyber resilience.

5.5 Framework Implementation

An organization can improve risk management by implementing this CSCD framework. Control sophistication level gives an understanding about implementing the approach of the specific risk. Controls can easily be implemented according to the RMM level. Specific organization can determine rules which are aligned with their business need and overall risk management capability. Risk management considerations include many aspects of cybersecurity, including the degree to which privacy and civil liberties considerations are integrated into an organization's cybersecurity risk management and potential risk responses (Barrett, 2018).

For any kind of framework implementation, it requires a process to follow. Enterprises face a lot of complexity and challenges to implementing a new process or framework. CSCD is a sensitive part for enterprises. Most enterprises follow the corporate governance model to implement a security framework. Carnegie Mellon University's Software Engineering Institute prepared a model to implement a framework according to their organizational structures. This model is known as the IDEAL model, where it describes: Initiating, Diagnosing, Establishing, Acting, and Learning (Poore, 2006).



I	**Initiating**	Lay the groundwork for a successful improvement effort.
D	**Diagnosing**	Determine where you are relative to where you want to be.
E	**Establishing**	Plan the specifics of how you will reach your destination.
A	**Acting**	Do the work according to the plan.
L	**Learning**	Learn from the experience and improve your ability to adopt new improvements in the future.

Figure 10: IDEAL model elaboration (Poore, 2006).

This phase included 15 activities. Though it was developed for software process improvement, now it can be used in cybersecurity (Poore, 2006). That means enterprises can follow IDEAL model to implement the CSCD framework.

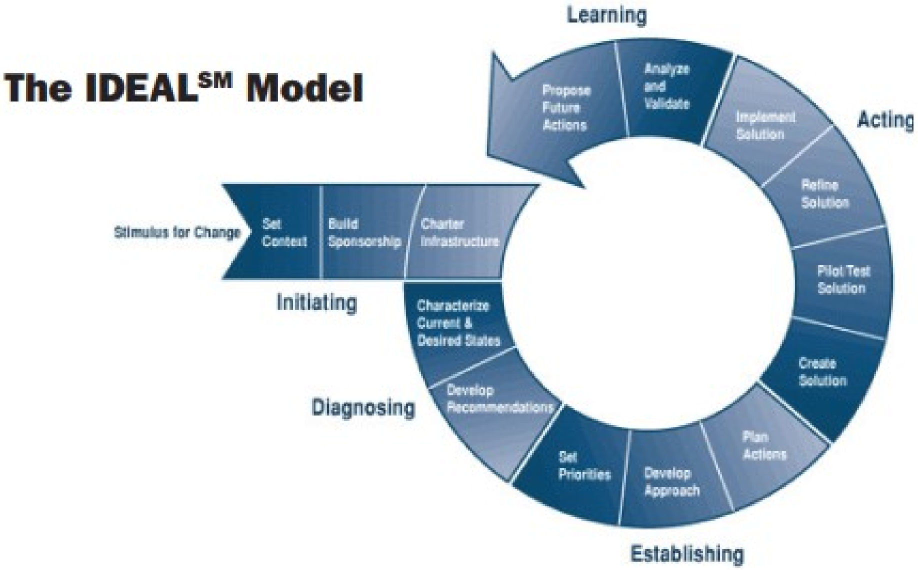


Figure 11: IDEAL model framework implementation (Poore, 2006).

This author (Poore, 2006) describes each segment of the IDEAL model. Here activities of each phase are going to explain accordingly. In the initial phase, simulate of changes means the changes which are needed. The next part is the level of risk acceptable to the organization where the organization can have a quick evaluation for the risk management process. All stakes understanding and agreement are required for changes and implementation, which led sponsor of the change initiative. Charter infrastructure defines the resources that will do actual activities.

A thorough assessment of the organization's security posture can characterize the current and desired stage of diagnosing phase. The recommendation can be placed after this assessment. Thirdly, in establishing phase, priorities can be set from the recommendation bases on criteria like business drivers, business area impact, and perhaps a recent risk assessment or audit. Based on the recommendations, a proper approach can be developed with an aspect of current skill set, maturity, capability, and actual requirement.

The acting phase is the actual implementation of the framework. Here test and refine the solution and later install or implement happen if all tests and refine validated and comply. Lastly, analysis and validation will be done along with proposing future action in the learning phase.

5.5.1 CSCD Governance

Cyber risk, security, and defense governance is a complex thing that required multi-function coordination. IT assets will be managed through CSCD governance involving different stakeholders. An effective CSCD governance system can improve threat identification, risk, and resource optimization. As CSCD management is a part of IT management, that is why we can do CSCD management and governance according to the way of IT management and governance. Governance ensures that stakeholder needs, conditions, and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved, setting direction through prioritization and decision making, and monitoring performance and compliance against agreed-on laws and objectives (Lanter, 2019). CSCD governance processes are the Information Security/Cybersecurity activities that support organizational goals. These main components of CSCD governance ensure that the confidentiality, integrity, and availability of an organization's electronic assets are maintained all the time, and information is never compromised (Von Solms, 2001). This also becomes a cyber-security governance concern if the information is transmitted via the internet. (Jennex & Zyngier, 2007) argue for the need for the organization to ensure that codified knowledge is recent and comprehensive, which again reflects the need for integrity. It is observed that (Johnston & Hale, 2009) confirmed empirically that the organizations that address their Information Security from the bottom up and isolate the governance from the management of IS have ineffective IS programs and can fall victim to internal and external cybersecurity attacks, in contrast to organizations whose CSCD governance programs have a proactive, top-down approach.

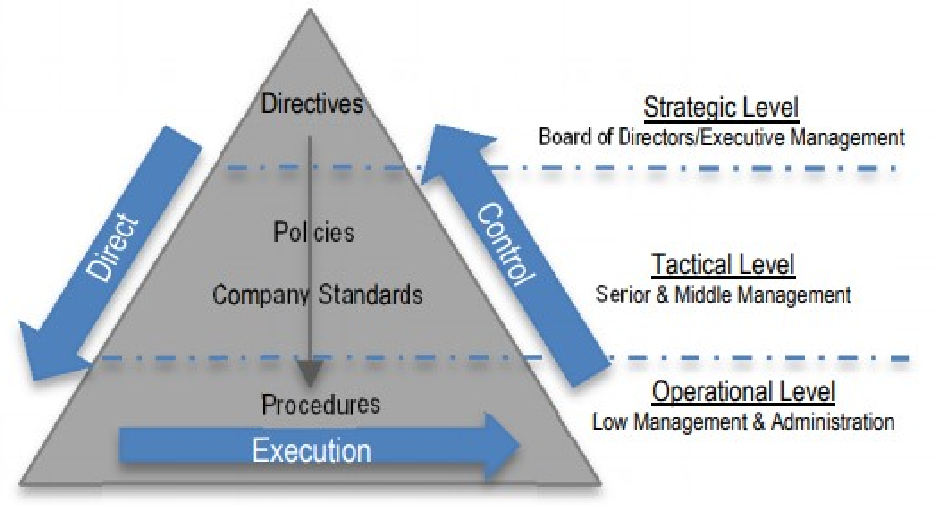


Figure 12: CSCD governance level (Gashgari et al., 2017).

So organizations can need to follow this model to maintain proper CSCD governance. Governance can be applied to the entire enterprise, an entity, a tangible or intangible asset, etc. It is possible to define different views of the enterprise to which governance is applied, and it is essential to define this scope of the governance system well (Lanter, 2019).

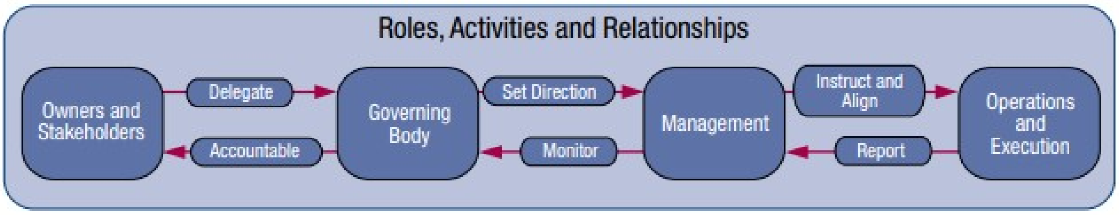


Figure 13: Roles, Activities, and Relationships interaction for CSCD governance (Lanter, 2019).

The author also clarifies element of governance roles, activities and relationships which defines who is involved in governance, how they are involved, what they do and how they interact, within the scope of any governance system. In COBIT 5, a clear differentiation is made between governance and management activities in the governance and management domains, as well as the interfacing between them and the role players that are involved.

5.6 CSCD Framework Component

In this part, a comprehensive view of the CSCD framework component will be elaborated. After analyzing several scientific frameworks and control documents, a set of criteria are defined for preparing control baseline and risk analysis.

5.6.1 CSCD Control Criteria

A set of criteria are the element to define the CSCD control plan. Based on that criteria, it would be well defined and structured to represent the CSCD guideline/control. Basically, in a greater sense, cybersecurity means IT asset security. It also means collecting tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets (International Telecommunication Union, 2008). After analyze and observation that most authors and leading papers (NIST, ISO) represented the CSCD control plan according to the asset. In this way, I represent my CSCD guideline control criteria like below according to the asset.

- Parent Control
- Sub Control
- Sub Control Detail
- IT Asset Type
- CSCD Function
- Sophistication Level
- RMM (Risk Management Maturity) Level
- Risk Level
    - Impact and Likelihood.

NIST defined a Cybersecurity framework based on Identify, Protect, Detect, Respond, and Recover, which are considered one of the structured frameworks (Barrett, 2018).

5.6.1.1 Parent Control Family

Parent control family has been designed based on different distinct focus areas of IT. Enterprises have different criticality in other functions according to their business nature. Despite that, the overall cybersecurity risk for all RMM level organizations is similar. Here, a list of leading parent control families is identified where all the control and risk level will be defined in a sub-category under this.

No	Parent Control Family	Trigram
1	Security Strategy and Planning	SSP
2	Policy, Business Continuity and compliance	PBC
3	Hardware Asset Management	HAM
4	Software Asset Management	SAM
5	Vulnerability Management	VM
6	Privileged Access Management	PAM
7	Identity, Access And Authentication Management	IAA
8	Configuration Management (Hardware, Software, Mobile device, laptop,	CM

	Workstation, servers, Iota, etc.)	
9	Maintenance, Monitoring and Log Management	MML
10	Email, Browser and Web Protections	EBW
11	Malware Defense Management	MDM
12	Limitation and Control of Network Ports, Protocols, and Services	LCN
13	Network Device Security (Firewall, Routers, Switch and etc.)	NDS
14	Network Defense	ND
15	Wireless Access Control	WAC
16	Data Protection, Recovery and Backup	DPR
17	Application Software Security	ASS
18	Risk Assessment and Management	RAM
19	Incident Response and Management	IRM
20	Penetration Tests and Red Team Exercises	PTR
21	Security Awareness and Training	SAT
22	External Service Management	ESM

Table 3: CSCD Parent Control Family

For data processing purposes, a short tri name is given to each control family so that it makes a straightforward representation of the result.

5.6.1.2 Sub Control

Sub controls are a set of controls under specific control family. Each sub-control is defined by the CSCD control function. Different enterprises are mapped under sub-control based on the RMM level. Actual control is described in this sub-control section.

5.6.1.3 Sub Control Detail

Each sub-control has a proper definition and elaboration in the sub-control detail section. Control implementation idea can be found from here.

5.6.1.4 IT Asset Type

IT asset is the essential part of this research because all the controls are defined based on specific asset types. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process (Barrett, 2018). Through the CSCD control measures, enterprises minimize the threats and risks. As because information associated with IT assets is typically voluminous, highly complex, and fast-changing, it is likely that organizations with such information will need to make use of automated information systems (ISO, 2017). After analyzing a number of scientific papers and frameworks, we defined the IT asset category, which gives a clear idea about different types of assets. In this way, it provides a comprehensive view to map, analyze and implement specific CSCD controls.

Asset Type	Detail	Source
Data	Any form of data, Database, DBMS , Bigdata,	(ISO, 2017), (NIST CSRC, 2021)
IT Hardware	Physical IT equipment: Servers, End users Devices, Network Devices, Switch, Firewall, Router, Communications equipment, IP, etc Physical Media Containing digital assets, including backups	(ISO, 2017). (ISO, 2017).
Software (Executable Code/Application)	Source code, API, Web services, Functional application, Web Browser, Software firewalls.	(ISO, 2017).
Software (Non-Executable Code/Application)	Fonts, Configurations, property files, binaries, servers configuration, Metadata, formulas, DataMart, etc.	(ISO, 2017).
Software (Virtual Equipment)	Firmware, virtual Machines, Embedded software	(ISO, 2017).
Digital Information Content	Digital assets with information content, e.g., documents, audio, video, graphics, free-standing dictionaries, etc.	(ISO, 2017).
IT Services	Combination of IT assets and non-IT assets, typically externally supplied, treated as IT assets, e.g., Software as a service, PAAS, IAAS hardware maintenance, training, etc. Wifi, Email	(ISO, 2017).
IT Contracts	Digital or physical contract document	(ISO, 2017).
IT Licenses	Digital and Physical license document	(ISO, 2017).
IT Platform	Operation systems, Computing Systems, Database platform, storage platform, mobile platform, storage platform, application platform, CMS platform, media platform, API platform, analytics platform, Security platform, robotics platform, IoT platform, AI platform, game platform, etc. Framework, Software development platform, tools, Block chain	(ISO, 2017).
Strategic assets	Policy, Process, Procedure Example of Policy: Application Access policy, Provision policy, Service threshold policy, etc. Example of the process : (App Dev Code Promotion, Maintenance, Change Management, Vulnerability Mgt, Account Setup, Account Maintenance New Client On boarding, Internal Audit, Device/System set-up, Customer Support). Documentation: UAT, User manual, IT process, IT policy, IT strategy, etc. Methodology, Training	(Kyengo & Kilika, 2017) (Kay, 2003)
Intangible assets	Intellectual property, digital trademarks, patents,	(Integration,

	copyright, Trade secrets, Franchises, Reputation, Brand, Goodwill	2007)
User	Personnel, End-user, Administrative user, Business user, Employee, Client, Customer, Developer, Any IT Asset user.	(ISO, 2017).
Organizational Asset	Organization	(ISO, 2017).
Non-IT Asset	Provider designation, Provide role, Communication Protocol	(ISO, 2017).
N/A	Not to categorize	
All	All types of Assets except Intangible assets, Non-IT assets, N/A	

Table 4: IT Asset Type

5.6.1.5 CSCD Framework Function:

The National Institute of Standards and Technology’s Cyber Security Framework organizes cybersecurity activities in five categories: Identify, Protect, Detect, Respond, and Recover. The recovery category differentiates this framework from all other frameworks. The NIST framework recognizes the importance of recovery planning and suggests the development, implementation, and maintenance of plans for timely recovering and restoring any capabilities or services that were impaired by a cyber-attack (Roure et al., 2019). This CSCD framework utilize this framework function model to define control categories and subcategories under specific function.

Identify
Protect
Detect
Respond
Recover

Figure 14: NIST cybersecurity framework function (Barrett, 2018).

(Barrett, 2018) describes perfectly in NIST framework about each function as like bellow. CSCD framework also adapts function specifications.

- **Identify**: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities (Barrett, 2018). Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs (Barrett, 2018).

• **Protect**: Develop and implement appropriate safeguards to ensure delivery of critical services where the Protect Function supports the ability to limit or contain a potential cybersecurity event (Barrett, 2018).

• **Detect**: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event (Barrett, 2018).

• **Respond**: Develop and implement appropriate activities to take action regarding a detected and the ability to contain the impact of a potential cybersecurity incident (Barrett, 2018).

• **Recover**: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident (Barrett, 2018).

5.6.1.6 CSCD Control Sophistication Level

According to (ENISA, 2016b) specification, Security measures are categorized into three sophistication levels like below. Each level contains the practices to assess the adequacy of the design and evidence that should be provided in order to check the effective implementation of the security practice (ENISA, 2016b).

No	SOPHISTICATION LEVEL	DESCRIPTION OF SOPHISITICATION LEVELS
1	Basic	- Basic security measures that could be implemented to reach the security objective - Examples that basic measures are in place
2	Industry standard	- Industry standard security measures to reach the objective and an ad-hoc review of the implementation, following changes or incidents. - Examples of Industry standard measures and evidence of reviews of the implementation reacting to changes and/or incidents.
3	State of the art	- State of the art (advanced) security measures, and continuous monitoring of implementation, structural review of implementation, taking into account changes, incidents, tests, and exercises, to proactively improve the implementation of security measures - Examples of state of the art (advanced) implementation, evidence of a structural review process, and evidence of pro-active steps to improve the implementation of security measures.

Table 5: CSCD control sophistication level (ENISA, 2016b).

5.6.1.7 Organizational CSCD Risk Management Maturity (RMM) Level

Implementation of CSCD guidelines is not easy for every type of organization. It requires skillful resources and adequate organizational culture. Based upon organizational resource and asset availability. There are different types of organization exist in the world and their IT asset, resources, CSCD tactics, Cyber Intelligence Capability are not in same level. Even some companies might have a limited number of resources, but the CSCD capability would be higher than other mid size enterprise. Mid or large organizations have the ability to enable the latest technologies, but the lack of proper use and knowledge of the technology, companies, may not implement the guidelines properly. Some authors defined the maturity of the organizations based upon some specified criteria. CSCD control guidelines implementations would be different from organization to organization. Measuring organizational maturity grade would be more effective for preparing guidelines and implement them to the *enterprises* (US Department of Homeland Security, 2014). Based upon some defined criteria collected from (Barrett, 2018), (CIS, 2019) and (ISO IEC, 2013), we prepare organizational CSCD Control Maturity level categorization like below.

Criteria	**Micro to Small (A)**	**Small to Medium (B)**	**Medium to Large (C)**	**Large to Super Large (D)**
Number of Employees	5 ≤ 500	501 ≤ 5000	5001 ≤ 50000	50001 ≤ 0.5M
Data Sensibility and Criticality (Financial, Personal, Health, Secrete data, etc.)	Very low to Low	Low to Medium Medium to High	High to Significant	High to Significant Significant to Extreme
Regulatory Compliance	Not able to Comply	Partially Comply	Partially Comply Fully Comply	Partially Comply Fully Comply
Brand Value	Low to Medium	Medium to High	High to Significant	Significant to Extreme
Cyber Security Expertise	Low to Medium	Medium to High	High to Significant	High to Significant
IT Expertise Resources	Very low to Low	Low to Medium	High to Significant	High to Significant Significant to Extreme
Company Asset (Hardware, Software, Data, People)	Limited	Moderate	Significant to Extreme	Significant to Extreme
CSCD Practice Adaption	Limited to Low	Low to Medium Medium to High	High to Significant	High to Significant
Integrated Governance	Low	Low to Medium Medium to High	Medium to High High to Significant	High to Significant Significant to Extreme
Enabling Technology	Low to Medium Medium to High	Medium to High High to Significant	Medium to High High to Significant	High to Significant Significant to Extreme
Research Centre	Limited to Low	Low to Medium Medium to High	Medium to High High to Significant	High to Significant Significant to Extreme
Process and Methodology Adaption	Limited to Low	Low to Medium Medium to High	Medium to High High to Significant	High to Significant Significant to Extreme
Quality and Risk Management	Limited to Low	Low to Medium Medium to High	Medium to High High to Significant	High to Significant Significant to Extreme
Cyber Intelligence Capability	Limited to Low	Low to Medium Medium to High	Medium to High High to Significant	High to Significant Significant to Extreme
Cyber Defense Capability (Active, Passive, Collaborative)	Limited to Low	Low to Medium Medium to High	Medium to High High to Significant	High to Significant Significant to Extreme
Digital Products	Limited to Low	Low to Medium Medium to High	Medium to High High to Significant	High to Significant Significant to Extreme
Dependency on Digital Platforms	Limited to Low	Low to Medium Medium to High	Medium to High High to Significant	High to Significant Significant to Extreme
Process Automation Enabling	Limited to Low	Low to Medium Medium to High	Medium to High High to Significant	High to Significant Significant to Extreme

Client/Customer impact (Financial, Reputational, Confidentiality, others) on Provided Services	Low to Medium Medium to High High to Significant	Low to Medium Medium to High High to Significant Significant to Extreme	Low to Medium Medium to High High to Significant Significant to Extreme	Low to Medium Medium to High High to Significant Significant to Extreme
Risk Management Process	-CSCD Risk management practice is Not formalized - Ad hoc risk manages Low CSCD priority -Prioritization of CSCD risk **may not be directly informed** by organizational Risk objectives, the threat environment, or business/mission requirements.	-CSCD Risk management practice is Approved but not established. -Prioritization of CSCD risk will be **directly informed** by organizational Risk objectives, the threat environment, or business/mission requirements.	-CSCD Risk management practice is Approved and expressed as policy. -Prioritization of CSCD risk will be **regularly informed** and **updated** by organizational Risk objectives, the threat environment, or business/mission requirements.	-CSCD Risk management practice is Approved and expressed based on previous and current CSCD activity and policy. -Prioritization of CSCD risk will be **regularly informed** and **updated** by advanced Cybersecurity technologies and practices.
Integrated Risk Management Program	-Limited CSCD Awareness at Organizational Level. -Irregular CSCD Risk Management implementation -No CSCD information-sharing process within the organization -CSCD risk assessment is not repeatable and reoccurring	-Limited to Low CSCD Awareness at Organizational Level. -Limited to Low CSCD Risk Management implementation. - Limited to Low or Informal CSCD information sharing process in few parts of the organization. -CSCD risk assessment is not repeatable and reoccurring	-Medium to High CSCD Awareness at Organizational Level. - Medium to High CSCD Risk management implementation. - Medium to High or formal CSCD information sharing process in few parts of the organization. -CSCD risk assessment is consistently and It is accurately monitoring regularly by appointed skillful resources with proper role and responsibility.	-High to Significant CSCD Awareness at Organizational Level. - High to Significant CSCD Risk management implementation. - High to Significant or formal CSCD information sharing process in few parts of the organization. -CSCD risk assessment is consistently and Accurately monitoring regularly financial and organizational risks by appointed handy resources with proper role and responsibility.
External Participation	-No Understanding of organizational role and ecosystem. - No collaboration among entities and stakeholders for information sharing. -Unaware of the cyber supply chain risks of the products and services.	-Limited to Low Understanding of organizational role and ecosystem. - Limited to Low collaboration among entities and stakeholders for information sharing. - Limited to Low awareness of the cyber supply chain risks of the products and services.	-Medium to High Understanding of organizational role and ecosystem. - Medium to High collaboration among entities and stakeholders for information sharing. - Medium to High awareness of the cyber supply chain risks of the products and services.	- High to Significant Understanding of organizational role and ecosystem. - High to Significant collaboration among entities and stakeholders for information sharing. - High to Significant awareness of the cyber supply chain risks of the products and services.

Table 6: CSCD Risk Management maturity Level enterprise category

5.6.1.8 CSCD Risk Analysis

CSCD risk assessment is very important for organizations. To better predict system vulnerabilities, cybersecurity researchers are developing new and more holistic approaches to characterizing cybersecurity system risk (King et al., 2018). Methods of cyber risk assessment attempt to address the challenges surrounding cybersecurity issues (Ganin et al., 2020). Determine the levels of cybersecurity risk that they are exposed to a good understanding of the risk levels would allow an organization to dedicate adequate action and resources to treat risks of the highest priority (CSA, 2019). Through the tools, an organization can assess the risks affecting its assets and what security controls and insurance decisions should be implemented to reduce the likelihood and/ or eventual impacts of cyber threats (Couce-Vieira et al., 2020).

Moreover, create a risk-aware culture within the organisation, and also, Risk assessment is an iterative process that involves engaging employees to think about technology risks and how they align to business objectives (CSA, 2019). Basically, risk assessment is a key component of a holistic, organization-wide *risk management process* (NIST, 2011)*. The author also provided illustrated view of the risk management process, which includes*: (i) framing risk; (ii) assessing risk; (iii) responding to risk, and (iv) monitoring risk*.*

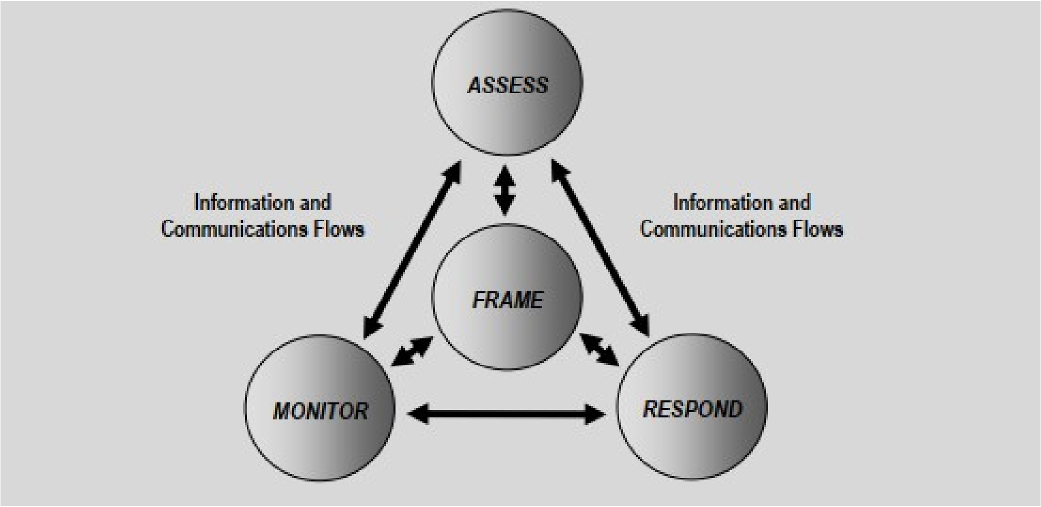

ASSESS
Information and Communications Flows
Information and Communications Flows
FRAME
MONITOR
RESPOND

Figure 15: Risk assessment within risk management process (NIST, 2011).

Moreover, enterprises get a much clear view of the level of risk management. (Kelley, 2014) illustrated the three-level of organization-wide risk management wherein level 1 includes Organization, Level 2 Mission and Business process, and level 3 includes system (Environment of operation). Security-related information goes bottom to top, and Risk tolerance & aggregated risk information goes top to bottom.

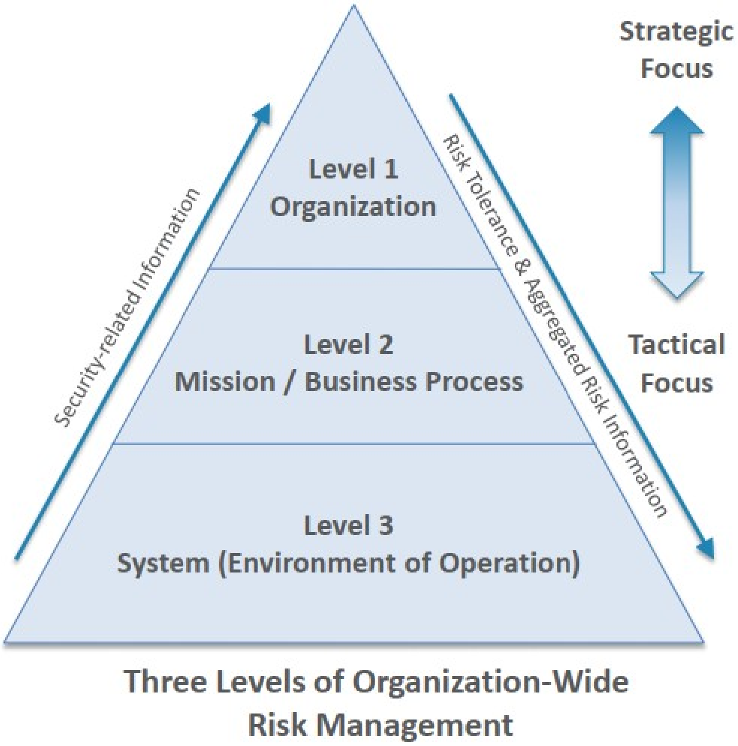

Strategic Focus
Tactical Focus
Level 1
Organization
Level 2
Mission / Business Process
Level 3
System (Environment of Operation)
Security-related Information
Risk Tolerance & Aggregated Risk Information
Three Levels of Organization-Wide Risk Management

Figure 16: Organization-wide risk management (Kelley, 2014).

For all kinds of strategic focus transmits level one towards level 3. All the tactical and gradual control relates risks will be managed at the system level. Here in this chapter, we will describe about the process of risk assessment along with risk framing, risk tolerance level, risk level criteria.

5.6.1.8.1 Risk Define Criteriaan Tolerance

We care about defining CSCD risk based on impact and likelihood.

Risk = Impact * Likelihood.

Here overall risk is defined based on the likelihood of a given threat event exercising on a vulnerability of an asset and the resulting impact of the occurrence of the threat event (CSA, 2019). Each of the risk factors mentioned in the definition is explained below.

Threat Event: Threat event refers to any event during which a threat actor, through threat vector, acts against an asset in a manner that has the potential to cause harm. In the context of cybersecurity, threat events can be characterized by the tactics, techniques, and procedures (TTP) employed by threat actors (CSA, 2019).

Vulnerability: Vulnerability refers to a weakness in the design, implementation, and operation of an asset or the internal control of a process (CSA, 2019).

Likelihood: Likelihood refers to the probability that a given threat event is capable of exploiting a shared vulnerability (or set of vulnerabilities). The possibility can be derived based on factors, namely, discoverability, exploitability, and reproducibility (CSA, 2019).

Impact: Impact refers to the magnitude of harm resulting from a threat event exploiting a vulnerability (or set of vulnerabilities). The magnitude of harm can be estimated from the perspective of a nation, organization, or individual (CSA, 2019).

According to the (CSA, 2019), we have defined risk level and tolerance description like below. In addition, we developed a risk tolerance level based on the calculated risk **score.**

Risk Level	Risk Tolerance Description	Tolerance Level
Very High (5)	This level of risk cannot be accepted and would create an impact so severe that the related activity would need to cease immediately. Alternatively, mitigation or transference strategies need to be taken immediately.	301≤ 375
High (4)	This level of risk cannot be accepted. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next one month.	226≤ 300
Medium High (3)	This level of risk cannot be accepted. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next 3-6 months.	151≤ 225
Medium (2)	This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be regularly monitored to ensure that any change in circumstance is detected and acted upon appropriately.	76≤ 150
Low (1)	This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be periodically monitored to ensure that any change in circumstances is detected and acted upon appropriately.	0≤ 75

Table 7: CSCD Risk Tolerance Level

Measuring Risk tolerance threshold level:

We have used a simple formula to calculate the risk tolerance threshold. Multiply of impact and likelihood create risk score of specific control. There are five criteria for measuring impact and three criteria for likelihood. Each criterion has one to five levels. For calculating impact or likelihood scores, every criterion can be specified by a specific level.

Impact Score Measurement							Likelihood Score Measurement			
Criterion	Confidentiality	Integrity	Availability	Strategic	Cross Level		Criterion	Reproducibility	Exploitability	Discoverability
Level							Level			
5	5	5	5	5	5	×	5	5	5	5
4	4	4	4	4	4		4	4	4	4
3	3	3	3	3	3		3	3	3	3
2	2	2	2	2	2		2	2	2	2
1	1	1	1	1	1		1	1	1	1

Table 8: Process of measuring impact and likelihood

That is how the total summation of impact / Likelihood score can be multiplied to get a risk score. Then risk level can be defined by the risk threshold matrix. As an example, for a specific control, we can assume the impact and likelihood score will be like below.

Impact Score Measurement							Likelihood Score Measurement			
Criterion	Confidentiality	Integrity	Availability	Strategic	Cross Level		Criterion	Reproducibility	Exploitability	Discoverability
Level							Level			
5	5	0	0	0	0	×	5	0	0	0
4	0	4	0	0	0		4	4	4	4
3	0	0	3	0	3		3	0	0	0
2	0	0	0	2	0		2	0	0	0
1	0	0	0	0	0		1	0	0	0

Table 9: Impact and likelihood score calculation

So we get an impact score 17 (5+4+3+2+3), and a Likelihood score is 12 (4+4+4). We will get a risk score If we now multiply both values. According to our example, the risk score is 204. According to the risk tolerance level, specific control can create medium-level risk for the organization if it has not been implemented.

Basically, the risk tolerance score is the multiply value of impact and likelihood score. According to this framework, the highest risk tolerance score is 375. The risk level is defined into five categories. We have used fair calculation to specify risk tolerance levels. As we have 5 risk levels and total multiplied value of impact and likelihood can be a maximum 375, we divide this maximum value with 5 to get per risk level value which is 75. Then we maintain per risk level by 75 compared to another risk level. That is how we can get risk tolerance levels from impact and likelihood scores, and finally, the risk level can find out for the specific control absent.

5.6.1.8.2 Determine Impact

Basically, the impact is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability (Swanson et al., 2010). With respect to security, the effect on organizational operations, organizational assets, individuals, other organizations, or the of loss of confidentiality, integrity, or availability of information or a system (NIST, 2018). As like (CSA, 2019), we have used CIA (confidentiality, integrity, availability) principal keys as one of the criteria for determining the impact of CSCD risk assessment. In NIST Cybersecurity Framework, the impact criteria are defined upon the Cybersecurity spectrum (Barrett, 2018).

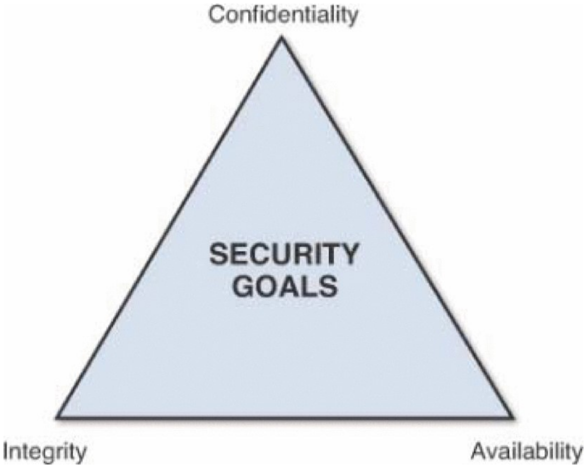


Figure 17: Information security model, the CIA triad (Al-Far et al., 2019)

Confidentiality: Confidentiality is the concept of ensuring that information is accessible for reading, listening, recording, or physical removal only to subjects entitled to it and that subjects only read or listens to the information to the extent permitted (Hammer & Schneider, 2007).

Integrity: Integrity refers to protecting information from being modified by unauthorized parties (NCES, 1998). According to (Cawthra et al., 2020), integrity is identifying, protecting, and responding to cyber threats and other destructive events. Maintaining adequate cybersecurity is crucial for a firm to maintain the integrity of its external and internal data, as well as to protect the firm's strategic proprietary information. Sharing cybersecurity-related information could also have impact on a firm's competitiveness on a particular market space (Gordon et al., 2015).

Availability: It means ensuring timely and reliable access to and use of information (Cawthra et al., 2020)

Apart from CIA, we have also included strategic and cross-level impact criteria.

Strategic Impact: Cyber vulnerabilities undermine confidence in strategic systems; they increase uncertainty in information and analysis, impacting the credibility of deterrence and strategic stability (Unal, 2019). The author also emphasizes that loss of trust in technology also has implications for attribution and strategic calculus in crisis decision-making and may increase the risk of misperception. Cybersecurity is not only creating an impact on IT asset but also have overall impact business. An organization's security strategy must be aligned with business strategy and integral to the senior leadership's decision-making process to ensure that risk is managed appropriately so organizations operate safely in the contemporary threat landscape (James, 2018). Moreover, in one study, 95% of business leaders acknowledged cyber-security as being an area of high importance, but 45% had no formal strategy in place around this (James, 2018). Organizations should rethink their approach to cyber-security now to protect shareholder interests and avoid upcoming sanctions (James, 2018). As digital technologies are strategically aligned with business strategy, the same should be done with cybersecurity (Spremić & Šimunic, 2018).

According to (Amit & Schoemaker, 1993) strategic assets are resource and capability which are scarce, uneasily traded, inimitable, durable and can be used to convert the value become profit. The strategic assets' characteristics imply that sources of sustainable competitive advantage are often related to intangible resources (Kyengo & Kilika, 2017). Intangible resources, also named knowledge, invisible assets, absorptive capabilities (Foss & Knudsen, 2003), core competencies, strategic assets, core capabilities (Galbreath, 2005), intellectual property rights, trademarks, information technology such as databases, networks, and skills such as capabilities and competencies(Lopez, 2001). (Bornemann & Leitner, 2002), observes that technology accumulated consumer information, brand name, reputation, and corporate culture are intangible assets that are invaluable to the firm's competitive power and also the only real source of competitive edge that can be sustained over time. Based on all the above references, we add new strategic impact in the criteria for measuring full impact score in risk assessment where disruption of achieving the strategic objective, competitiveness, sustain value, quality, and excellence are the main key elements.

Cross Level Impact: Multinational corporations (MNCs) want to locate their facilities in regions with characteristics that best suit their needs where the primary consideration is economic cost minimization (Escalante & Maier-Speredelozzi, 2008). This author (Lse et al., 2019) explains how and why multinational corporations have global footprints. Hence, one of the manifestations of the increasing diversity in multinational corporation (MNC) operations is the growing importance of regional headquarters (RHQs). RHQs assume an intermediary, bridging role between the corporate headquarters and local affiliates and other actors in their respective regions (Commission & Affairs, 2006). We also get a strong idea from this author about the cross-level location of MNC, which are departmental, organizational, regional, national, and Global.

On the other hand (CSA, 2019) considers national, organizational, and individual criteria for determining impact. From a large corporation's perspective, the effect can happen at different levels like departmental or regional levels. That is why we consider cross-level criteria with varying levels of layering according to the location model to identify a more accurate impact for CSCD. These cross-level criteria are Individual, Department, Branch, Region, National, Global, and Organizational.

Impact detection criteria and respective rating values are bellowed.

Impact Criteria	**Confidentiality**	**Integrity**	**Availability**	**Strategic**	**Cross Level**
Impact Rating					
Very Severe (5)	Unauthorized access and/or misuse of information are responsible for making an exceptionally significant effect.	Unauthorized Alteration of information is responsible for making an exceptionally significant effect.	Disruption of access/ service to authorized users of IT Assets is responsible for making exceptionally significant effects.	Disruption of achieving the strategic objective, competitiveness, sustain value, quality, and excellence are responsible for making an exceptionally significant effect.	Individual Department Branch Region Nation Global Organization
Severe (4)	Unauthorized access and/or misuse of information are responsible for making a serious adverse effect.	Unauthorized Alteration of information is responsible for making a serious adverse effect.	Disruption of access/ service to authorized users of IT Assets is responsible for making a serious adverse effect.	Disruption of achieving the strategic objective, competitiveness, sustain value, quality, and excellence are responsible for making a serious adverse effect.	Individual Department Branch Region Nation Organization
Moderate (3)	Unauthorized access and/or misuse of information are responsible for making some adverse effects.	Unauthorized Alteration of information is responsible for making some adverse effects.	Disruption of access/ service to authorized users of IT Assets is responsible for making some adverse effects.	Disruption of achieving the strategic objective, competitiveness, sustain value, quality, and excellence are responsible for making some adverse effects.	Individual Department Branch Region
Minor (2)	Unauthorized access and/or misuse of	Unauthorized Alteration of information is	Disruption of access/ service to authorized	Disruption of achieving the strategic	Individual Department Branch

	information are responsible for making limited adverse effects.	responsible for making limited adverse effects.	users of IT Assets is responsible for making a limited adverse effect.	objective, competitiveness, sustain value, quality, and excellence are responsible for limiting adverse effects.	
Negotiable (1)	Unauthorized access and/or misuse of information are responsible for making minor adverse effects.	Unauthorized Alteration of information is responsible for making a minor adverse effect.	Disruption of access/ service to authorized users of IT Assets is responsible for making minor adverse effects.	Disruption of achieving the strategic objective, competitiveness, sustain value, quality, and excellence are responsible for making minor adverse effects.	Individual Department

Table 10: CSCD Impact criteria (CSA, 2019) (Cronin, 2018)**,** (Thayer et al., 2013)

5.6.1.8.3 Determine Likelihood

Risk likelihood is the measurement metric of the historical or expected occurrence of an event (CSA, 2019). The degree to which a threat is expected to create an impact which stated in terms of frequency, foreseeability, or probability (Cronin, 2018). To determine the likelihood of an undesired state, the possible reasons for its occurrence have to be assessed regarding issues like the probability of accidents or regarding cyberattack know-how, equipment, vulnerabilities of the target, and so on (Kiesling et al., 2016). For measuring the dynamic nature of cybersecurity threats, we will use a likelihood measurement system. In this research, we use the following factors to identify CSCD risk likelihood.

Discoverability - How easy would an adversary be able to discover the vulnerability of an asset? This is dependent on the availability of information about the vulnerability and the exposure of the vulnerable asset (CSA, 2019).

Exploitability - How easy would an adversary exploit the vulnerability of an asset? This is dependent on the access rights, complexity of tools, as well as technical skills required to carry out the attack (CSA, 2019).

Reproducibility - How easy would an adversary be able to reproduce the attack on the asset? This is dependent on the complexity of the exploit customization and the environmental conditions required to carry out the attack (CSA, 2019).

Likelihood Criteria	Reproducibility	Exploitability	Discoverability
Likelihood Rating			
High Likely (5)	• Attack can occur anytime.	• Less possible to detect attack/threat by CTI based on OCM level. • Very easily exploit the vulnerability to the IT asset.	• Not discovered vulnerability
Likely (4)	• Attack can usually occur.	• Limited possibility to detect attack/threat by CTI based on OCM level. • Easily exploit the vulnerability to the IT asset.	• Few parts of vulnerabilities are discovered
Possible (3)	• Attack is expected to occur but not usually.	• Reasonable possibility to detect attack/threat by CTI based on OCM level. • Moderately exploit the vulnerability to the IT asset.	• Some parts of vulnerabilities are discovered
Unlikely (2)	• Attack is foreseeable to occur but not repetitively.	• Advance possibility to detect attack/threat by CTI based on OCM level. • Limitedly exploit the vulnerability to the IT asset.	• Most parts of vulnerabilities are discovered
Rare (1)	• Attack is not Foreseeable to occur.	• High possibility to detect attack/threat by CTI based on OCM level. • Very limitedly exploit the vulnerability to the IT asset.	• Full parts of vulnerabilities are discovered

Table 11: Likelihood criteria (CSA, 2019) (Cronin, 2018) (Thayer et al., 2013)

5.7 CSCD CONTROL BASELINE

In this part, the CSCD control guideline will be presented. Based upon the defined criteria above, we have designed control based like according to parent control family. As the controls of each family are aligned and mapped from the different frameworks, it will be easy for enterprises to implement CSCD control along with strategic planning to safeguard IT assets.

5.7.1. Security Strategy and Planning Control Family

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
1.1	Strategic assets	N/A	Basic	Develop and Maintain SECURITY PLANNING POLICY AND PROCEDURES	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	2
					4 - Large to Super Large	2
1.2	Strategic assets	Identify	Basic	Develop and Maintain SYSTEM SECURITY PLAN	1 - Micro to Small	2
					2 - Small to Medium	2

					3 - Medium to Large	2
					4 - Large to Super Large	2
1.3	Organizational Asset	N/A	Basic	COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	2 - Small to Medium	2
					3 - Medium to Large	2
					4 - Large to Super Large	2
1.4	All	Identify	Basic	Develops an information security architecture for the information system	2 - Small to Medium	2
					3 - Medium to Large	2
					4 - Large to Super Large	2
1.5	Non-IT Asset	N/A	Basic	Structure of security roles and responsible item is regularly reviewed and revised, based on changes and/or past incidents.	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	2
					6 - Large to Super Large	2

Table 12: Security Strategy and Planning Control Family

5.7.2 Policy, Business Continuity, and compliance

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
2.1	Strategic assets	Identify	Industry standard	Set a high level security policy	1 - Micro to Small	2
					2 - Small to Medium	2
					3 - Medium to Large	2
					4 - Large to Super Large	2
2.2	Strategic assets	Identify	Industry standard	Set detailed information security policies for critical assets and business processes.	1 - Micro to Small	2
					2 - Small to Medium	2
					3 - Medium to Large	2
					4 - Large to Super Large	2
2.3	Strategic assets	Identify	Industry standard	Review the information security/Cybersecurity policies periodically	1 - Micro to Small	1
					2 - Small to Medium	2
					3 - Medium to Large	2
					4 - Large to Super Large	2
2.4	User	N/A	Basic	Make all personnel aware of the security policy and what it entails for their work.	1 - Micro to Small	2
	Strategic assets				2 - Small to Medium	2
					3 - Medium to Large	2
					4 - Large to Super Large	2
2.5	User	Identify	Basic	Perform background checks/screening for key personnel and external contractors, when needed and legally permit ted.	3 - Medium to Large	2
					4 - Large to Super Large	2
2.6	User	Identify	Industry standard	Set up a policy and procedure for background checks.	3 - Medium to Large	2

	Strategic assets				4 - Large to Super Large	2
2.7	Strategic assets	N/A	Basic	Review and update policy/procedures for background checks and reference checks at regular intervals, taking into account changes and past incidents.	3 - Medium to Large	1
					4 - Large to Super Large	1
2.8	Non-IT Asset	Identify	Basic	Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	2
					4 - Large to Super Large	2
2.9	IT Hardware	Identify	Industry standard	A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.	3 - Medium to Large	2
	Strategic assets				4 - Large to Super Large	2
2.10	User	Identify	Basic	A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.	3 - Medium to Large	2
	Strategic assets				4 - Large to Super Large	2

Table 13: Policy, Business Continuity, and compliance Control Family

5.7.3. Hardware Asset Management

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
3.1	IT Hardware	Identify	Basic	Maintain Detailed Asset Inventory of Physical devices and systems within the organization.	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	1
					4 - Large to Super Large	1
3.2	IT Hardware	Identify	Basic	Maintain Asset Inventory Information	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	1
					4 - Large to Super Large	1
3.3	IT Hardware	Identify	Basic	External information systems are catalogued	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	1
					4 - Large to Super Large	1
3.4	IT Hardware	Identify	Basic	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and	1 - Micro to Small	1
					2 - Small to Medium	1

				business value	3 - Medium to Large	1
					4 - Large to Super Large	1
3.5	IT Hardware	Identify	Basic	Utilize discovery tool for active and passive asset	3 - Medium to Large	1
					4 - Large to Super Large	1
3.6	IT Hardware	Identify	Basic	Use DHCP Logging to Update Asset Inventory	3 - Medium to Large	1
					4 - Large to Super Large	1
3.7	IT Hardware	Respond	Basic	Address Unauthorized Assets	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	2
					4 - Large to Super Large	2
3.8	IT Hardware	Protect	Basic	Deploy Port Level Access Control	3 - Medium to Large	4
					4 - Large to Super Large	4
3.9	IT Hardware	Protect	Basic	Utilize Client Certificates Authentication mechanism Hardware Assets	4 - Large to Super Large	4
3.10	IT Hardware	Protect	Industry standard	Maintain Alternate Storage Site and Separation from Primary Site	3 - Medium to Large	3
					4 - Large to Super Large	3
3.11	IT Hardware	Protect	Industry standard	Alternate Processing Site	3 - Medium to Large	3
					4 - Large to Super Large	3
3.12	IT Hardware	Protect	State of the art	Separate Storage for Critical Information	2 - Small to Medium	3
					3 - Medium to Large	4
					4 - Large to Super Large	4
3.13	IT Hardware	Protect	State of the art	Protect power equipment and power cabling	3 - Medium to Large	5
					4 - Large to Super Large	5
3.14	IT Hardware	Protect	State of the art	Maintain Redundant Cabling	3 - Medium to Large	3
					4 - Large to Super Large	3
3.15	IT Hardware	Protect	State of the art	Maitain Automatic Voltage Controls	3 - Medium to Large	5
					4 - Large to Super Large	5
3.16	IT Hardware	Protect	State of the art	Emergency Shutoff	2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5
3.17	IT Hardware	Protect	State of the art	Emergency Power	1 - Micro to Small	3
					2 - Small to Medium	4

					3 - Medium to Large	4
					4 - Large to Super Large	4
3.18	IT Hardware	Protect	State of the art	Ensure Alternate Power Supply for Minimal Operational Capability	2 - Small to Medium	3
					3 - Medium to Large	4
					4 - Large to Super Large	4
3.19	IT Hardware	Protect	Industry standard	Emergency Lighting	3 - Medium to Large	1
					4 - Large to Super Large	1
3.20	IT Hardware	Protect	Industry standard	Protect Against Unauthorized Physical Connections	3 - Medium to Large	5
					4 - Large to Super Large	5

Table 14: Hardware Asset Management Control Family

5.7.4. Software Asset Management

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
4.1	Software (Executable Code/Application) Software (Virtual Equipment) IT Platform	Identify	Basic	Maintain Inventory of Software platforms and applications within the organization.	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	1
					4 - Large to Super Large	1
4.2	Software (Executable Code/Application) Software (Non-Executable Code/Application) IT Platform IT Services	Identify	Basic	Ensure Software update and support by Vendor	1 - Micro to Small	2
					2 - Small to Medium	2
					3 - Medium to Large	4
					4 - Large to Super Large	4
4.3	Software (Executable Code/Application) Software (Non-Executable Code/Application) Software (Virtual Equipment)	Identify	Basic	Utilize Software Inventory Tools	3 - Medium to Large	1
					4 - Large to Super Large	1
4.4	Software (Executable Code/Application) Software (Non-Executable Code/Application) Software (Virtual	Identify	Basic	Track Software Inventory Information	3 - Medium to Large	1
					4 - Large to Super Large	1

	Equipment)					
	IT Services					
	IT Platform					1
4.5	Software (Executable Code/Application)	Identify	Basic	Integrate Software and Hardware Asset Inventories	3 - Medium to Large	1
	Software (Non-Executable Code/Application)				4 - Large to Super Large	1
	Software (Virtual Equipment)					
	IT Services					1
	IT Platform					1
4.6	Software (Executable Code/Application)	Respond	Basic	Address and Removed Unapproved Software	1 - Micro to Small	5
	Software (Non-Executable Code/Application)				2 - Small to Medium	5
	Software (Virtual Equipment)				3 - Medium to Large	5
	IT Services				4 - Large to Super Large	5
	IT Platform					
4.7	Software (Executable Code/Application)	Protect	Basic	Utilize Application Whitelisting Technology	4 - Large to Super Large	5
	Software (Non-Executable Code/Application)					
	Software (Virtual Equipment)					
	IT Services					
	IT Platform					
4.8	Software (Executable Code/Application)	Protect	Basic	Implement Application Whitelisting of Libraries	4 - Large to Super Large	5
	Software (Non-Executable Code/Application)					
	Software (Virtual Equipment)					
	IT Services					
	IT Platform					
4.9	Software (Executable Code/Application)	Protect	Basic	Implement Application Whitelisting of Scripts	4 - Large to Super Large	5
	Software (Non-Executable Code/Application)					
	Software (Virtual Equipment)					
	IT Services					
	IT Platform					
4.10	Software (Executable Code/Application)	Protect	Basic	Physically or Logically Segregate High Risk Applications	4 - Large to Super Large	3
	Software (Non-Executable					

	Code/Application)					
	Software (Virtual Equipment)					
	IT Services					
	IT Platform					
4.11	Software (Executable Code/Application)	Protect	Industry standard	Restriction on Software usuage	1 - Micro to Small	1
	Software (Non-Executable Code/Application)				2 - Small to Medium	1
	Software (Virtual Equipment)				3 - Medium to Large	2
	IT Services				4 - Large to Super Large	2
	IT Platform					
4.12	Software (Executable Code/Application)	Protect	State of the art	Use Automatic mechanisms for software updates	2 - Small to Medium	1
	Software (Non-Executable Code/Application)				3 - Medium to Large	2
	IT Services				4 - Large to Super Large	2
	IT Platform					
	Software (Executable Code/Application)	Detect	State of the art	Maintain notification Before or After update Softeware or OS	2 - Small to Medium	2
4.13	Software (Non-Executable Code/Application)				3 - Medium to Large	3
	Software (Virtual Equipment)				4 - Large to Super Large	3
	IT Services					
	IT Platform					
4.14	IT Hardware	Protect	State of the art	(IoT specific control): Verify the authenticity and integrity of each update via a trust relationship	2 - Small to Medium	5
	Software (Executable Code/Application)				3 - Medium to Large	5
					4 - Large to Super Large	5

Table 15: Software Asset Management Control Family

5.7.5. Vulnerability Management

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
5.1	Software (Executable Code/Application)	Detect	Basic	Identify and Document Asset Vulnerability	3 - Medium to Large	1
	Software (Non-Executable					

	Code/Application) Software (Virtual Equipment) IT Services IT Platform IT Hardware					
					4 - Large to Super Large	1
5.2	Software (Executable Code/Application) Software (Non-Executable Code/Application) Software (Virtual Equipment) IT Services IT Platform IT Hardware	Detect	Basic	Perform Authenticated Vulnerability Scanning	3 - Medium to Large	2
					4 - Large to Super Large	2
5.3	Software (Executable Code/Application) Software (Non-Executable Code/Application) Software (Virtual Equipment) IT Services IT Platform IT Hardware	Protect	Basic	Perform vulnerability with Protect Dedicated Assessment Accounts	3 - Medium to Large	1
					4 - Large to Super Large	1
5.4	IT Platform	Protect	Basic	Deploy Automated Operating System Patch Management Tools	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	2
					4 - Large to Super Large	4
5.5	Software (Executable Code/Application) Software (Non-Executable Code/Application) Software (Virtual Equipment) IT Services IT Platform IT Hardware	Protect	Basic	Utilize Automated Software Patch Management Tools	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	2
					4 - Large to Super Large	2
5.6	Software (Executable Code/Application) Software (Non-Executable	Respond	Basic	Compare Back-to-Back Vulnerability Scans	3 - Medium to Large	1

	Code/Application) Software (Virtual Equipment)					
	IT Services IT Platform IT Hardware				4 - Large to Super Large	1
5.7	Software (Executable Code/Application) Software (Non-Executable Code/Application) Software (Virtual Equipment)	Identify	Industry standard	Subscribe to vulnerability intelligence services	3 - Medium to Large	2
	IT Services IT Platform IT Hardware				4 - Large to Super Large	2

Table 16: Vulnerability Management Control Family

5.7.6. Privileged Accounts Management

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
6.1	User	Detect	Basic	Maintain Inventory of Administrative Accounts	3 - Medium to Large	2
					4 - Large to Super Large	2
6.2	User	Identify	Basic	Define Group and role Membership	2 - Small to Medium	1
					3 - Medium to Large	1
					4 - Large to Super Large	1
6.3	User	Protect	Industry standard	Maintain Automatic and dynamic System of Account Management	3 - Medium to Large	2
					4 - Large to Super Large	3
6.4	User	Protect	Basic	Change Default Password	1 - Micro to Small	4
					2 - Small to Medium	4
					3 - Medium to Large	4
					4 - Large to Super Large	4
6.5	User	Protect	Basic	Ensure the Use of Dedicated Administrative Accounts	1 - Micro to Small	4
					2 - Small to Medium	4
					3 - Medium to Large	4
					4 - Large to Super Large	4
6.6	User	Protect	Basic	Use Unique Passwords	1 - Micro to Small	4
					2 - Small to Medium	4

					3 - Medium to Large	4
					4 - Large to Super Large	4
6.7	User	Protect	Basic	Use Multi-Factor Authentication for All Administrative Access	3 - Medium to Large	4
					4 - Large to Super Large	4
6.8	User	Protect	Basic	Use Dedicated Workstations For All Administrative Tasks	4 - Large to Super Large	4
6.9	User	Protect	Basic	Limit Access to Scripting Tools	3 - Medium to Large	4
					4 - Large to Super Large	4
6.10	User	Detect	Basic	Log and Alert on Changes to Administrative Group Membership	3 - Medium to Large	4
					4 - Large to Super Large	4
6.11	User	Detect	Basic	Log and Alert on Unsuccessful Administrative Account Login	3 - Medium to Large	4
					4 - Large to Super Large	4
6.12	User	Detect	Industry standard	Automate Account Management Audit	3 - Medium to Large	1
					4 - Large to Super Large	2
6.13	User	Detect	Industry standard	Establish Priviledge Accounts Monitoring process	3 - Medium to Large	4
					4 - Large to Super Large	4
6.14	User	Protect	Industry standard	Establish Role Based Access Control	2 - Small to Medium	2
					3 - Medium to Large	4
					4 - Large to Super Large	4
6.15	User	Protect	Industry standard	Review of User Privileges	3 - Medium to Large	1
					4 - Large to Super Large	2
6.16	User	Protect	Industry standard	Enforce Limit of Unsuccessful Logon Attempts	2 - Small to Medium	2
					3 - Medium to Large	2
					4 - Large to Super Large	2
6.17	User	Protect	Industry standard	Maintain System Notification	2 - Small to Medium	1
					3 - Medium to Large	2

					4 - Large to Super Large	2
6.18	User	Respond	Industry standard	Block access to a machine (either remotely or locally) for administratorlevel accounts.	2 - Small to Medium	4
					3 - Medium to Large	4
					4 - Large to Super Large	4

Table 15: Privileged Accounts Management Control Family

5.7.7. Identity, Access, and Authentication Management

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
7.1	User	Identify	Basic	Maintain an Inventory of Authentication Systems	3 - Medium to Large	1
					4 - Large to Super Large	1
7.2	User	Protect	Industry standard	Maintain Automatic and dynamic System of Account Management	3 - Medium to Large	2
					4 - Large to Super Large	3
7.3	User	Protect	State of the art	Configure Centralized Point of Authentication	3 - Medium to Large	3
					4 - Large to Super Large	3
7.4	User	Protect	State of the art	Utilize Multi-Factor Authentication	3 - Medium to Large	4
					4 - Large to Super Large	4
7.5	User	Protect	Industry standard	Encrypt or Hash All Authentication Credentials	2 - Small to Medium	4
					3 - Medium to Large	4
					4 - Large to Super Large	4
7.6	User	Protect	Industry standard	Encrypt Transmittel of Username and Authentication Credentials	3 - Medium to Large	4
					4 - Large to Super Large	4
7.7	User	Identify	Industry standard	Maintain an Inventory of Accounts	3 - Medium to Large	1
					4 - Large to Super Large	1
7.8	User	Protect	Industry standard	Establish Process for Revoking Access	3 - Medium to Large	1
					4 - Large to Super Large	1
7.9	User	Respond	Industry standard	Disable Any Unassociated Accounts	1 - Micro to Small	4
					2 - Small to Medium	4
					3 - Medium to Large	4
					4 - Large to Super Large	4
7.10	User	Respond	Industry standard	Maintain Disable Accounts policy	1 - Micro to Small	1

					2 - Small to Medium	1
					3 - Medium to Large	2
					4 - Large to Super Large	2
7.11	User	Protect	Basic	Ensure All Accounts Have An Expiration Date	1 - Micro to Small	2
					2 - Small to Medium	2
					3 - Medium to Large	4
					4 - Large to Super Large	4
7.12	User	Protect	Basic	Lock Workstation Sessions After Inactivity	1 - Micro to Small	2
					2 - Small to Medium	2
					3 - Medium to Large	3
					4 - Large to Super Large	3
7.13	User	Detect	Industry standard	Monitor Attempts to Access Deactivated Accounts	3 - Medium to Large	3
					4 - Large to Super Large	3
7.14	User	Detect	Industry standard	Alert on Account Login Behavior Deviation	4 - Large to Super Large	3
7.16	User	Protect	Basic	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	1 - Micro to Small	4
					2 - Small to Medium	4
					3 - Medium to Large	4
					4 - Large to Super Large	4
7.17	User	Protect	Basic	Remote access is managed	3 - Medium to Large	4
					4 - Large to Super Large	4
7.18	User	Protect	Industry standard	Monitoring and Control of Remote Access	3 - Medium to Large	4
					4 - Large to Super Large	4
7.19	User	Protect	Industry standard	Authorize Privileged Commands and Access of Remote Access	3 - Medium to Large	4
					4 - Large to Super Large	4
7.20	User	Protect	Industry standard	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	3 - Medium to Large	4
					4 - Large to Super Large	4
7.21	IT Hardware Software (Virtual Equipment) Digital Information Content IT Services IT Platform User	Protect	Basic	Network integrity is protected (e.g., network segregation, network segmentation)	3 - Medium to Large	4
					4 - Large to Super Large	4
7.22	User	Detect	State of the art	Automate Account Management Audit	3 - Medium to Large	2
					4 - Large to Super Large	2
7.23	User	Protect	State of the art	Establish Dynamic Priviledge	3 - Medium to Large	2

				Management	4 - Large to Super Large	2
7.24	User	Protect	Industry standard	Establish Role Based Access Control	2 - Small to Medium	4
					3 - Medium to Large	4
					4 - Large to Super Large	4
7.25	User	Protect	Industry standard	Restrict Access to Specific Information Types	2 - Small to Medium	4
					3 - Medium to Large	4
					4 - Large to Super Large	4
7.26	User	Protect	Industry standard	Maintain Domain Authentication	4 - Large to Super Large	2
7.27	User	Protect	Industry standard	Maintain Least Privilege	2 - Small to Medium	4
					3 - Medium to Large	4
					4 - Large to Super Large	4
7.28	User	Protect	Industry standard	Review of User Privileges	3 - Medium to Large	2
					4 - Large to Super Large	2
7.29	User	Protect	Basic	Enforce Limit of Unsuccessful Logon Attempts	2 - Small to Medium	4
					3 - Medium to Large	4
					4 - Large to Super Large	4
7.30	User	Protect	Industry standard	Maintain System Notification	2 - Small to Medium	2
					3 - Medium to Large	2
					4 - Large to Super Large	2
7.31	User	Protect	Industry standard	Limit Concurrent Session	3 - Medium to Large	2
					4 - Large to Super Large	2
7.32	User	Protect	Industry standard	Employ envryption for Mobile Device to Control Access	4 - Large to Super Large	4
7.33	IT Hardware	Protect	Basic	Restricted Use of Non-organizationally Owned and Portable Storage Devices	3 - Medium to Large	4
					4 - Large to Super Large	4
7.34	User	Protect	State of the art	Maintain Single Sign-on	2 - Small to Medium	3
					3 - Medium to Large	3
					4 - Large to Super Large	3

7.35	User	Protect	Industry standard	Dynamic Address Allocation	3 - Medium to Large	3
					4 - Large to Super Large	3
7.36	User	Protect	Basic	Maintain Password-based Authentication	1 - Micro to Small	4
					2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5
7.37	User	Protect	State of the art	Maintain Public Key-based Authentication	3 - Medium to Large	4
					4 - Large to Super Large	4
7.38	User	Protect	State of the art	Maintain token-based Authentication	3 - Medium to Large	4
					4 - Large to Super Large	4
7.39	User	Protect	Industry standard	Bind identities and authenticators dynamically	4 - Large to Super Large	2
7.40	User	Protect	Industry standard	Maintain Identification and Authentication non orgirizational User	2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5
7.41	User	Protect	Industry standard	Maintain Identity Proofing by Supervisor Authorization	2 - Small to Medium	4
					3 - Medium to Large	5
					4 - Large to Super Large	5
7.42	User	Protect	Basic	Restrict Publicly Accecible Content	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	2
					4 - Large to Super Large	2
7.43	User	Protect	State of the art	Cross Organizational Credential Management	3 - Medium to Large	2
					4 - Large to Super Large	2

7.44	User	Protect	Industry standard	Maintain strong password policy	1 - Micro to Small	4
					2 - Small to Medium	4
					3 - Medium to Large	4
					4 - Large to Super Large	4
7.45	User	Detect	Industry standard	Monitor access to network and in formation systems, have a process for approving exceptions and regis tering access violations	3 - Medium to Large	2
					4 - Large to Super Large	2
7.46	Strategic assets	Identify	Industry standard	Evaluate the effectiveness of access control policies and procedures and implement cross checks on access control mechanisms.	3 - Medium to Large	1
					4 - Large to Super Large	1
7.47	User	Protect	State of the art	For Bigdata Perspective: Use trusted certificates	3 - Medium to Large	4
					4 - Large to Super Large	4
7.48	User	Protect	Industry standard	For Cloud Perspective: automatically update access control lists (ACLs) or traffic flow policies	1 - Micro to Small	4
					2 - Small to Medium	4
7.49	User User	Protect Protect	Industry standard State of the art	For Cloud Perspective: automatically update access control lists (ACLs) or traffic flow policies Broken authentication and session management	3 - Medium to Large	4
					4 - Large to Super Large	4
					3 - Medium to Large	3
					4 - Large to Super Large	3
7.50	User	Protect	State of the art	Dual Authorization for Deletion or Destruction	2 - Small to Medium	4
					3 - Medium to Large	4
7.51	User	Protect	State of the art	Dual Authorization for Deletion or Destruction	4 - Large to Super Large	4

Table 17: Identity, Access, and Authentication Management Control Family

5.7.8. Configuration Management (Hardware, Software, Mobile device, laptop, Workstation, servers, IoT, etc.)

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
8.1	Software (Executable Code/Application)	Protect	Basic	Establish Secure Configurations	1 - Micro to Small	2
					2 - Small to Medium	5
	Software (Non-Executable Code/Application)				3 - Medium to Large	5
	Software (Virtual Equipment)					
	IT Platform				4 - Large to Super Large	5
	IT Services					
8.2	Software (Executable Code/Application)	Protect	Industry standard	Maintain Secure Images	3 - Medium to Large	5
	Software (Non-Executable Code/Application)					
	Software (Virtual Equipment)				4 - Large to Super Large	5
	IT Services					
	IT Platform					
8.3	Software (Executable Code/Application)	Protect	Industry standard	Securely Store Master Images	3 - Medium to Large	1
	Software (Non-Executable Code/Application)					
	Software (Virtual Equipment)				4 - Large to Super Large	1
	IT Services					
	IT Platform					
8.4	Software (Executable Code/Application)	Protect	Industry standard	Deploy System Configuration Management Tools automatically	3 - Medium to Large	2
	Software (Non-Executable Code/Application)					
	Software (Virtual Equipment)				4 - Large to Super Large	2
	IT Services					
	IT Platform					
8.5	Software (Executable Code/Application)	Detect	Industry standard	Implement Automated Configuration	3 - Medium to Large	2

	Software (Non-Executable Code/Application)			Monitoring Systems		
	Software (Virtual Equipment)				4 - Large to Super Large	2
	IT Services					
	IT Platform					
8.6	Software (Executable Code/Application)	Detect	Industry standard	Utilize file integrity checking tools	2 - Small to Medium	1
	Software (Non-Executable Code/Application)				3 - Medium to Large	2
	Digital Information Content				4 - Large to Super Large	2

Table 18: Configuration Management Control Family

5.7.9. Maintenance, Monitoring, and Log Management

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
9.1	IT Hardware	Detect	Basic	Utilize Three Synchronized Time Sources	3 - Medium to Large	4
	IT Services					
	Software (Executable Code/Application)				4 - Large to Super Large	4
	IT Platform					
9.2	IT Hardware	Detect	Basic	Activate Audit Logging	2 - Small to Medium	1
	IT Services				3 - Medium to Large	2
	Software (Executable Code/Application)					
	IT Platform				4 - Large to Super Large	2
9.3	IT Hardware	Detect	Basic	Enable Detailed Logging	3 - Medium to Large	2
	IT Services				4 - Large to Super Large	2
	Software (Executable Code/Application)					
	IT Platform					
9.4	IT Hardware	Detect	Basic	Ensure Adequate Storage for Logs	3 - Medium to Large	2
	IT Services					
	IT Platform				4 - Large to Super Large	2

9.5	IT Hardware IT Services Software (Executable Code/Application) IT Platform	Detect	Industry standard	Central Log Management	3 - Medium to Large 4 - Large to Super Large	2 2
9.6	IT Hardware IT Services Software (Executable Code/Application) IT Platform Software (Non-Executable Code/Application) Software (Virtual Equipment) Software (Executable Code/Application) IT Platform	Detect	Industry standard	Deploy SIEM or Log Analytic Tools	2 - Small to Medium 3 - Medium to Large 4 - Large to Super Large	2 4 4
9.7	IT Hardware Software (Executable Code/Application) Software (Non-Executable Code/Application) Software (Virtual Equipment) IT Services IT Platform	Identify	Industry standard	Regularly Review, Analysis, and Reporting Logs and notifications	3 - Medium to Large 4 - Large to Super Large	1 1
9.8	IT Hardware IT Services IT Platform Software (Executable Code/Application) Software (Non-Executable Code/Application) Software (Virtual Equipment)	Detect	Industry standard	Regularly Tune SIEM	4 - Large to Super Large	2
9.9	IT Hardware IT Services IT Platform Software (Executable Code/Application) Software (Non-Executable Code/Application) Software (Virtual Equipment)	Protect	Industry standard	Store on Separate Physical Systems or Components for Protecting Audit Information	4 - Large to Super Large	1
9.10	IT Hardware	Protect	Basic	Prevent Unauthorized Removal of maintenance tool	3 - Medium to Large 4 - Large to Super Large	2 2
9.11	IT Hardware	Protect	Industry standard	Monitoring Physical	2 - Small to Medium	3

				Access to Systems	3 - Medium to Large	5
					4 - Large to Super Large	5
9.12	IT Hardware	Protect	Basic	Maintain Visitor Access Records	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	2
					4 - Large to Super Large	2
9.13	Strategic assets	Identify	Basic	Develop a log retention policy to make sure that the logs are kept for a sufficient period of time.	2 - Small to Medium	1
					3 - Medium to Large	1
					4 - Large to Super Large	1
9.14	Data	Identify	Industry standard	For Bigdata Perspective: Mine logging events	3 - Medium to Large	2
	IT Platform				4 - Large to Super Large	2
9.15	IT Services	Protect	State of the art	For Cloud Perspective: platform should support API security and tenant isolation of VMs/containers	2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5
9.15	IT Services	Detect	State of the art	For Cloud Perspective: Host antivirus and malicious code prevention	2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5
9.16	IT Services	Protect	State of the art	For Cloud Perspective: API Security	2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5

Table 19: Maintenance, Monitoring, and Log Management Control Family

5.7.10. Email, Browser, and Web Protections

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
10.1	Software (Executable Code/Application)	Protect	Basic	Ensure that only fully supported web browsers	1 - Micro to Small	2
					2 - Small to Medium	2
					3 - Medium to Large	4
					4 - Large to Super Large	4
10.2	Software (Executable Code/Application)	Protect	Basic	Disable Unnecessary or Unauthorized Browser or Email Client Plugins	2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5

10.3	Software (Executable Code/Application)	Protect	Industry standard	Limit Use of Scripting Languages in Web Browsers and Email Clients	3 - Medium to Large	3
					4 - Large to Super Large	3
10.4	Software (Executable Code/Application)	Protect	Industry standard	Maintain and Enforce Network-Based URL Filters	3 - Medium to Large	3
					4 - Large to Super Large	4
	IT Hardware					1
10.5	Software (Executable Code/Application)	Protect	Industry standard	Subscribe to URL Categorization Service	3 - Medium to Large	4
	IT Hardware				4 - Large to Super Large	1
10.6	Software (Executable Code/Application)	Detect	Industry standard	Log All URL Requests	3 - Medium to Large	2
	IT Hardware				4 - Large to Super Large	3
10.7	Software (Executable Code/Application)	Protect	State of the art	Use of DNS Filtering Services	2 - Small to Medium	2
	IT Hardware				3 - Medium to Large	2
					4 - Large to Super Large	4
10.8	Software (Executable Code/Application)	Protect	State of the art	Implement DMARC and Enable Receiver-Side Verification	3 - Medium to Large	4
	IT Hardware				4 - Large to Super Large	4
10.9	IT Hardware	Protect	Industry standard	Block Unnecessary File Types	3 - Medium to Large	4
	Software (Executable Code/Application)				4 - Large to Super Large	4
10.10	Software (Executable Code/Application)	Protect	Industry standard	Sandbox All Email Attachments	4 - Large to Super Large	4
	IT Hardware					
10.11	Software (Executable Code/Application)	Detect	State of the art	Activity monitoring	4 - Large to Super Large	5
	IT Hardware					
10.12	IT Services	Detect	Industry standard	For Cloud Perspective: Host intrusion detection and prevention	1 - Micro to Small	2
					2 - Small to Medium	2
		Protect			3 - Medium to Large	3
					4 - Large to Super Large	3

Table 20: Email, Browser, and Web Protections Control Family

5.7.11. Malware Defense Management

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
11.1	IT Hardware	Protect	Industry standard	Utilize Centrally Managed Anti-Malware	3 - Medium to Large	5
	Software					

	(Executable Code/Application)			Software		
	IT Services				4 - Large to Super Large	5
	IT Platform					
11.2	IT Hardware	Protect	Industry standard	Ensure Anti-Malware Software and Signatures Are Updated	1 - Micro to Small	4
	Software (Executable Code/Application)				2 - Small to Medium	5
	IT Services				3 - Medium to Large	5
	IT Platform				4 - Large to Super Large	5
11.3	IT Hardware	Detect	State of the art	Enable Operating System Anti-Exploitation Features/ Deploy Anti Exploit Technologies	3 - Medium to Large	5
	IT Platform				4 - Large to Super Large	5
11.4	IT Hardware	Detect	Basic	Configure Anti-Malware Scanning of Removable Media	1 - Micro to Small	5
					2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5
11.5	IT Hardware	Protect	Basic	Configure Devices to Not Auto-Run Content	1 - Micro to Small	5
					2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5
11.6	IT Hardware	Detect	Industry standard	Centralize Anti-Malware Logging	3 - Medium to Large	2
					4 - Large to Super Large	2
11.7	IT Hardware	Detect	State of the art	Enable DNS Query Logging	3 - Medium to Large	4
					4 - Large to Super Large	4
			State of the art	Enable Command-Line Audit Logging	3 - Medium to Large	3
					4 - Large to Super Large	4
11.8	IT Hardware	Detect	Core	Unauthorized mobile code, OTP, Token are detected	3 - Medium to Large	5
					4 - Large to Super Large	5
11.9	IT Services	Detect	Basic	Scan email and filter webcontent	1 - Micro to Small	5
					2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5
11.10	Data	Protect	Industry standard	Enable anti-exploitation features	3 - Medium to Large	2
					4 - Large to Super Large	4
11.11	Software (Executable Code/Application)	Identify	State of the art	Use network-based anti-malware tools to identify executables	2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5
11.12	All	Respond	Basic	Implement an incident response process that allows the IT support	3 - Medium to Large	2
					4 - Large to Super Large	3

				organization to supply the security team with samples of malware		

Table 21: Malware Defense Management

5.7.12. Limitation and Control of Network Ports, Protocols, and Services

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
12.1	IT Hardware	Identify	Basic	Associate Active Ports, Services, and Protocols to Asset Inventory	3 - Medium to Large	2
					4 - Large to Super Large	2
12.2	IT Hardware	Protect	Basic	Ensure Only Approved Ports, Protocols, and Services Are Running	3 - Medium to Large	5
					4 - Large to Super Large	5
12.3	IT Hardware	Detect	Basic	Perform Regular Automated Port Scans	3 - Medium to Large	4
					4 - Large to Super Large	4
12.4	IT Hardware	Protect	Industry standard	Apply Host-Based Firewalls or Port-Filtering	1 - Micro to Small	3
					2 - Small to Medium	3
					3 - Medium to Large	5
					4 - Large to Super Large	5
12.5	IT Hardware	Protect	State of the art	Implement Application Firewalls	4 - Large to Super Large	5
12.6	IT Hardware	Detect	Industry standard	Verify any server that is visible from the Internet or an untrusted network	2 - Small to Medium	5
	IT Services				3 - Medium to Large	5
	IT Platform				4 - Large to Super Large	5
	Data					1
12.7	IT Hardware	Protect	Industry standard	Operate critical services on separate physical or logical host machines	2 - Small to Medium	4
	IT Services				3 - Medium to Large	4
	IT Platform				4 - Large to Super Large	5
12.8	IT Services	Protect	State of the art	For Cloud Perspective: limit the maximum traffic of the management network	1 - Micro to Small	5
					2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5
				Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security	2 - Small to Medium	1
12.9	Strategic assets	Identify	Basic		3 - Medium to Large	1
					4 - Large to Super Large	2

				features implemented for those protocols considered to be insecure		
12.10	IT Hardware	Protect	State of the art	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	2 - Small to Medium	4
	Data				3 - Medium to Large	4
	IT Platform				4 - Large to Super Large	5
	IT Services					1
12.11	IT Hardware	Respond	State of the art	Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.	2 - Small to Medium	3
					3 - Medium to Large	4
					4 - Large to Super Large	5
12.12	User	Protect	Basic	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network	1 - Micro to Small	5
					2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5
12.13	IT Hardware	Protect	Basic	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers	2 - Small to Medium	5
	Software (Executable Code/Application)				3 - Medium to Large	5
	IT Services				4 - Large to Super Large	5
	IT Platform					5

Table 22: Limitation and Control of Network Ports, Protocols, and Services Control Family

5.7.13. Network Device Security (Firewall, Routers, Switch and etc.)

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
13.1	IT Hardware	Identify	Industry standard	Maintain Standard Security Configurations for Network Devices	3 - Medium to Large	5
					4 - Large to Super Large	5
13.2	IT Hardware	Identify	Basic	Document Traffic Configuration Rules	3 - Medium to Large	3
					4 - Large to Super Large	4
13.3	IT Hardware	Detect	Industry standard	Use Automated Tools to Verify Standard Device Configurations and Detect Changes	3 - Medium to Large	5
					4 - Large to Super Large	5
13.4	IT Hardware	Protect	Industry standard	Install the Latest Stable Version of Any	1 - Micro to Small	5
					2 - Small to Medium	5

				Security Related Updates on All Network Devices	3 - Medium to Large	5
					4 - Large to Super Large	5
13.5	IT Hardware	Protect	State of the art	Manage Network Devices Using Multi Factor Authentication and Encrypted Sessions	3 - Medium to Large	5
					4 - Large to Super Large	5
13.6	IT Hardware	Protect	Basic	Use Dedicated Workstations for All Network Administrative Tasks	3 - Medium to Large	4
					4 - Large to Super Large	5
13.7	IT Hardware	Protect	Industry standard	Manage Network Infrastructure Through a Dedicated Network	3 - Medium to Large	5
					4 - Large to Super Large	5
13.8	IT Hardware	Protect	Industry standard	Secure and synchronize router configuration files.	1 - Micro to Small	3
					2 - Small to Medium	4
					3 - Medium to Large	5
					4 - Large to Super Large	5
13.9	IT Hardware	Protect	State of the art	Install perimeter firewalls	2 - Small to Medium	4
					3 - Medium to Large	4
					4 - Large to Super Large	4

Table 23: Network Device Security (Firewall, Routers, Switch and etc.) Control Family

5.7.14. Network Defense

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
14.1	IT Hardware	Identify	Basic	Maintain an Inventory of Network Boundaries	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	1
					4 - Large to Super Large	1
14.2	IT Hardware	Detect	State of the art	Scan for Unauthorized Connections Across Trusted Network Boundaries	3 - Medium to Large	4
					4 - Large to Super Large	5
14.3	IT Hardware	Protect	Industry standard	Deny Communications With Known Malicious IP Addresses	3 - Medium to Large	5
					4 - Large to Super Large	5

14.4.	IT Hardware	Protect	State of the art	Deny Communication Over Unauthorized Ports	1 - Micro to Small	5
					2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5
14.5	IT Hardware	Detect	State of the art	Configure Monitoring Systems to Record Network Packets	3 - Medium to Large	5
					4 - Large to Super Large	5
14.6	IT Hardware	Detect	State of the art	Deploy Network-Based IDS Sensors	3 - Medium to Large	3
					4 - Large to Super Large	3
14.7	IT Hardware	Protect	State of the art	Deploy Network-Based Intrusion Prevention Systems	4 - Large to Super Large	5
14.8	IT Hardware	Detect	State of the art	Deploy NetFlow Collection on Networking Boundary Devices	3 - Medium to Large	2
					4 - Large to Super Large	4
14.9	IT Hardware	Detect	State of the art	Deploy Application Layer Filtering Proxy Server	4 - Large to Super Large	4
14.10	IT Hardware	Detect	State of the art	Decrypt Network Traffic at Proxy	4 - Large to Super Large	4
14.11	User	Detect	State of the art	Require All Remote Logins to Use Multi Factor Authentication	3 - Medium to Large	5
					4 - Large to Super Large	5
14.12	IT Hardware	Protect	Industry standard	Manage All Devices Remotely Logging Into Internal Network	4 - Large to Super Large	4
14.13	IT Hardware	Protect	Industry standard	Segment the Network Based on Sensitivity	3 - Medium to Large	2
					4 - Large to Super Large	4
14.14	IT Hardware	Protect	Industry standard	Disable Workstation to-Workstation Communication	3 - Medium to Large	4
					4 - Large to Super Large	5
14.15	IT Hardware	Protect	Industry standard	Enable Firewall Filtering Between VLANs	3 - Medium to Large	4
					4 - Large to Super Large	4
14.16	IT Hardware	Protect	State of the art	Restrict Ability to Attack Other Systems	2 - Small to Medium	5
	IT Services				3 - Medium to Large	5
	IT Platform				4 - Large to Super Large	5
14.17	IT Hardware	Protect	State of the art	Detection and Monitoring	2 - Small to Medium	5
	IT Services				3 - Medium to Large	5
	IT Platform				4 - Large to Super Large	5
14.18	IT Hardware	Protect	State of the art	Maintain Networked Privileged Accesses	3 - Medium to Large	5
	IT Services				4 - Large to Super Large	5
14.19	IT Hardware	Protect	Industry standard	Block Communication from Non-organizationally Configured Hosts	3 - Medium to Large	5

	IT Services				4 - Large to Super Large	5
14.20	IT Hardware	Protect	State of the art	Separate Subnets for Connecting to Different Security Domains	1 - Micro to Small	4
	IT Services				2 - Small to Medium	4
	IT Platform				3 - Medium to Large	4
	Data				4 - Large to Super Large	4
14.21	IT Services	Protect	Industry standard	Disable Sender Feedback on Protocol Validation Failure	2 - Small to Medium	2
	User				3 - Medium to Large	3
	IT Platform				4 - Large to Super Large	3
14.22	IT Hardware	Protect	State of the art	Allow DMZ systems to communicate with private network systems	3 - Medium to Large	4
	IT Services				4 - Large to Super Large	5
14.23	Software (Executable Code/Application)	Protect	State of the art	Make sure software of network and information systems is not tampered with or altered, for instance by using input controls.	1 - Micro to Small	5
	Software (Virtual Equipment)				2 - Small to Medium	5
	IT Services				3 - Medium to Large	5
	IT Platform				4 - Large to Super Large	5
14.24	IT Hardware	Protect	State of the art	For Bigdata Perspective: Use transport layer security (TLS) to establish connections and communication	3 - Medium to Large	5
	IT Services				4 - Large to Super Large	5
14.25	IT Hardware	Protect	State of the art	Secure isolation of multi-tenant network services is required	1 - Micro to Small	5
	IT Services				2 - Small to Medium	5
	IT Platform				3 - Medium to Large	5
					4 - Large to Super Large	5
14.26	IT Hardware	Protect	State of the art	Design the network using a minimum of a three-tier architecture (DMZ, middleware, and private network).	3 - Medium to Large	5
					4 - Large to Super Large	5
14.27	IT Hardware	Respond	Industry standard	Rapid response and shunning of detected attacks	3 - Medium to Large	5
					4 - Large to Super Large	5
14.28	IT Hardware	Protect	Industry standard	Deploy domain name systems (DNS) in a hierarchical, structured fashion	3 - Medium to Large	2
					4 - Large to Super Large	2
14.29	IT Hardware	Protect	State of the art	Segment the enterprise network into multiple, separate trust zones	3 - Medium to Large	2
					4 - Large to Super Large	3

Table 24: Network Defense Control Family

5.7.15. Wireless Access Control

After analyzing numbers of scientific research paper and CSCD control frameworks from here following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
15.1	IT Hardware	Identify	Basic	Maintain an Inventory of Authorized Wireless Access Points	3 - Medium to Large	2
					4 - Large to Super Large	2
15.2	IT Hardware	Detect	Basic	Detect Wireless Access Points Connected to the Wired Network	3 - Medium to Large	2
					4 - Large to Super Large	2
15.3	IT Hardware	Detect	Industry standard	Use a Wireless Intrusion Detection System	3 - Medium to Large	4
					4 - Large to Super Large	4
15.4	IT Hardware	Protect	Basic	Disable Wireless Access on Devices if Not Required	4 - Large to Super Large	2
15.5	IT Hardware	Protect	Basic	Limit Wireless Access on Client Devices	4 - Large to Super Large	2
15.6	IT Hardware	Protect	Industry standard	Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients	3 - Medium to Large	2
					4 - Large to Super Large	3
15.7	IT Hardware	Protect	State of the art	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	1 - Micro to Small	2
					2 - Small to Medium	2
					3 - Medium to Large	3
					4 - Large to Super Large	4
15.8	IT Hardware	Protect	Industry standard	Use Wireless Authentication Protocols That Require Mutual, Multi-Factor Authentication	4 - Large to Super Large	4
15.9	IT Hardware	Protect	Basic	Disable Wireless Peripheral Access to Devices	4 - Large to Super Large	4
15.10	IT Hardware	Protect	Basic	Create Separate Wireless Network for Personal and Untrusted Devices	1 - Micro to Small	2
					2 - Small to Medium	2
					3 - Medium to Large	3
					4 - Large to Super Large	3
15.11	IT Hardware	Protect	Industry standard	Restrict Configurations by Users	3 - Medium to Large	3
					4 - Large to Super Large	3
15.12	IT Hardware	Protect	Industry standard	Ensure that each wireless device connected to the network matches an authorized configuration and security profile	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	2
					4 - Large to Super Large	3
15.13	IT Hardware	Protect	Industry standard	Install personal firewall software or equivalent functionality on any portable computing devices	3 - Medium to Large	2
					4 - Large to Super Large	3

Table 25: Wireless Access Control

5.7.16. Data Protection, Recovery, and Backup

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
16.1	Data	Identify	Basic	Maintain an Inventory of Sensitive Information	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	1
					4 - Large to Super Large	1
16.2	Data	Protect	Basic	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	1 - Micro to Small	2
					2 - Small to Medium	2
					3 - Medium to Large	4
					4 - Large to Super Large	4
16.3	Data	Detect	State of the art	Monitor and Block Unauthorized Network Traffic	4 - Large to Super Large	5
16.4	Data	Protect	Basic	Only Allow Access to Authorized Cloud Storage or Email Providers	3 - Medium to Large	4
					4 - Large to Super Large	4
16.5	Data	Detect	State of the art	Monitor and Detect Any Unauthorized Use of Encryption	4 - Large to Super Large	5
16.6	Data	Protect	Industry standard	Encrypt Mobile Device Data	4 - Large to Super Large	3
16.7	Data	Protect	Basic	Manage USB Devices	3 - Medium to Large	4
	IT Hardware				4 - Large to Super Large	5
16.8	Data	Protect	Basic	Manage System's External Removable Media's Read/Write Configurations	4 - Large to Super Large	4
16.9	Data	Protect	Basic	Encrypt Data on USB Storage Devices	4 - Large to Super Large	3
16.10	Data	Protect	State of the art	Encrypt All Sensitive Information in Transit	3 - Medium to Large	5
					4 - Large to Super Large	5
16.11	Data	Detect	State of the art	Utilize an Active Discovery Tool to Identify Sensitive Data	4 - Large to Super Large	4
16.12	Data	Protect	State of the art	Protect Information Through Access Control Lists	1 - Micro to Small	5
					2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5
16.13	Data	Protect	Industry standard	Enforce Access Control to Data Through Automated Tools	4 - Large to Super Large	5
16.14	Data	Protect	State of the art	Encrypt all sensitive information at rest using a tool that requires a secondary	4 - Large to Super Large	3

				authentication		
16.15	Data	Detect	Industry standard	Enforce Detail Logging for Access or Changes to Sensitive Data	4 - Large to Super Large	3
16.16	Data	Protect	State of the art	ENFORCE PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS	3 - Medium to Large	3
					4 - Large to Super Large	5
16.17	Data	Protect	State of the art	For IoT Perspective Encript user data	2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5
16.18	Data	Protect	State of the art	Ensure that each system is automatically backed up	1 - Micro to Small	2
					2 - Small to Medium	2
					3 - Medium to Large	5
					4 - Large to Super Large	5
16.19	Data	Protect	Industry standard	Test data on backup media on a regular basis	2 - Small to Medium	2
					3 - Medium to Large	3
					4 - Large to Super Large	4
16.20	Data	Protect	Industry standard	Ensure that key systems have at least one backup destination that is not continuously addressable	2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5
16.21	Data	Protect	State of the art	For Bigdata Perspective : Prevent information leakage through output	3 - Medium to Large	5
					4 - Large to Super Large	5
16.22	Data	Protect	State of the art	For Bigdata Perspective: Ensure data replication consistency	3 - Medium to Large	3
					4 - Large to Super Large	4
16.23	Data	Protect	Industry standard	For Bigdata Perspective: Utilize policy-based encryption system (PBES7)	3 - Medium to Large	2
					4 - Large to Super Large	2
16.24	Data	Recover	State of the art	Implement mediated decryption system	3 - Medium to Large	5
					4 - Large to Super Large	5
16.25	Data	Protect	Industry standard	For Bigdata Perspective: Limit features of homomorphic encryption for practical implementation	3 - Medium to Large	2
					4 - Large to Super Large	2
16.26	Data	Protect	State of the art	For Bigdata Perspective: Utilize attribute-based encryption and access control	3 - Medium to Large	2
					4 - Large to Super Large	5
16.27	Data	Protect	State of the art	For Cloud Perspective: User data on different VMs is isolated at the virtualization	1 - Micro to Small	2
					2 - Small to Medium	2
					3 - Medium to Large	3
					4 - Large to Super Large	4
16.28	Data	Protect	Industry standard	Separate Physical or Logical flow of Information	4 - Large to Super Large	2
16.29	Data	Protect	State of the art	Validation of Metadata	4 - Large to Super Large	2
16.30	Data	Detect	Industry standard	Sanitize Data	4 - Large to Super Large	4

16.31	Data	Protect	Industry standard	Perform Complete System Backups	1 - Micro to Small	2
					2 - Small to Medium	3
					3 - Medium to Large	5
					4 - Large to Super Large	5
16.32	Data	Protect	Industry standard	Test Data on Backup Media	2 - Small to Medium	2
					3 - Medium to Large	2
					4 - Large to Super Large	2
16.33	Data	Protect	Industry standard	Protect Backups	1 - Micro to Small	3
					2 - Small to Medium	3
					3 - Medium to Large	5
					4 - Large to Super Large	5
16.34	Data	Protect	Industry standard	Ensure All Backups Have at Least One Offline Backup Destination	1 - Micro to Small	2
					2 - Small to Medium	2
					3 - Medium to Large	3
					4 - Large to Super Large	3

Table 26: Data Protection, Recovery, and Backup Control Family

5.7.17. Application Software Security

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
17.1	Software (Executable Code/Application)	Protect	Industry standard	Establish Secure Coding Practices	3 - Medium to Large	3
	User				4 - Large to Super Large	5
17.2	Software (Executable Code/Application)	Identify	Industry standard	Ensure That Explicit Error Checking Is Performed for All In-House Developed Software	3 - Medium to Large	2
	User				4 - Large to Super Large	3
17.3	Software (Executable Code/Application)	Identify	Industry standard	Verify That Acquired Software Is Still Supported	3 - Medium to Large	5
	Software (Non-Executable Code/Application)				4 - Large to Super Large	5
	Software (Virtual Equipment)					1
17.4	Software (Executable Code/Application)	N/A	Industry standard	Only Use Up-to-Date and Trusted Third-Party Components	4 - Large to Super Large	5
	Software (Non-Executable Code/Application)					
	Software (Virtual Equipment)					
	IT Services					
	IT Platform					
17.5	Software (Executable	N/A	Basic	Use only Standardized and Extensively	3 - Medium to Large	2

	Code/Application)			Reviewed Encryption Algorithms		
	Software (Non-Executable Code/Application)				4 - Large to Super Large	3
17.6	User	N/A	Basic	Ensure Software Development Personnel Are Trained in Secure Coding	3 - Medium to Large	2
					4 - Large to Super Large	2
17.7	Software (Executable Code/Application)	N/A	State of the art	Apply Static and Dynamic Code Analysis Tools	3 - Medium to Large	2
	Software (Non-Executable Code/Application)				4 - Large to Super Large	2
17.8	Strategic assets	N/A	Industry standard	Establish a Process to Accept and Address Reports of Software Vulnerabilities	3 - Medium to Large	2
					4 - Large to Super Large	2
17.9	IT Platform	N/A	Industry standard	Separate Production and Non-Production Systems	3 - Medium to Large	3
					4 - Large to Super Large	3
17.10	Software (Executable Code/Application)	N/A	State of the art	Deploy Web Application Firewalls	3 - Medium to Large	5
					4 - Large to Super Large	5
17.11	Data	N/A	Industry standard	Use Standard Hardening Configuration Templates for Databases	3 - Medium to Large	2
					4 - Large to Super Large	3
17.12	Software (Executable Code/Application)	Protect	Basic	Restriction usage of Open-source Software	3 - Medium to Large	3
	IT Platform				4 - Large to Super Large	5
17.13	Software (Non-Executable Code/Application)	Protect	Basic	User-installed Software	3 - Medium to Large	2
	IT Platform				4 - Large to Super Large	2
17.14	Software (Executable Code/Application)	Protect	State of the art	Automated Enforcement and Monitoring	3 - Medium to Large	3
	IT Platform				4 - Large to Super Large	4
17.15	Software (Executable Code/Application)	Protect	State of the art	Dynamic Code Analysis	3 - Medium to Large	2
	Software (Non-Executable Code/Application)				4 - Large to Super Large	2
17.16	Software (Executable Code/Application)	Protect	State of the art	Interactive Application Security Testing	3 - Medium to Large	3
	Software (Non-Executable Code/Application)				4 - Large to Super Large	4
17.17	Software (Executable Code/Application)	Protect	State of the art	Security and Privacy Tracking Tools for Development Process, Standards, and Tools	3 - Medium to Large	4
	Software (Non-Executable Code/Application)				4 - Large to Super Large	5
17.18	Software (Executable Code/Application)	Protect	State of the art	Automated Vulnerability Analysis for Development Process, Standards, and Tools	3 - Medium to Large	3
	Software (Non-Executable Code/Application)				4 - Large to Super Large	4

17.19	Software (Executable Code/Application) Software (Non-Executable Code/Application) IT Services	Identify	Industry standard	Structure for Testing	2 - Small to Medium 3 - Medium to Large 4 - Large to Super Large	2 2 2
17.20	Software (Executable Code/Application) Software (Non-Executable Code/Application)	Protect	State of the art	Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system.	3 - Medium to Large 4 - Large to Super Large	5 5
17.21	Software (Executable Code/Application) IT Platform IT Services Data	Protect	Basic	Stop displaying system error messages to end-users	1 - Micro to Small 2 - Small to Medium 3 - Medium to Large 4 - Large to Super Large	2 2 3 3
17.22	Software (Executable Code/Application) Software (Non-Executable Code/Application) Software (Virtual Equipment) IT Services IT Platform	Protect	Industry standard	Examine the product security process of the vendor	1 - Micro to Small 2 - Small to Medium 3 - Medium to Large 4 - Large to Super Large	2 2 3 3 3
17.23	Data Software (Executable Code/Application) Software (Non-Executable Code/Application) Software (Virtual Equipment) IT Services	Protect	Industry standard	Use standard hardening configuration templates for DB	1 - Micro to Small 2 - Small to Medium 3 - Medium to Large 4 - Large to Super Large	2 2 3 4 1
17.24	Data IT Services Software (Executable Code/Application)	Protect	State of the art	For Bigdata Perspective: :Maintain worker nodes	1 - Micro to Small 2 - Small to Medium 3 - Medium to Large 4 - Large to Super Large	2 2 2 2
17.25	Data	Detect	State of the art	For Bigdata Perspective: Detect fake nodes	1 - Micro to Small 2 - Small to Medium 3 - Medium to Large 4 - Large to Super Large	5 5 5 5

Table 27: Application Software Security control Control Family

5.7.18. Risk Assessment and Management

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
18.1	All	Detect	State of the art	Use of All-source Intelligence	3 - Medium to Large	4
					4 - Large to Super Large	4
18.2	User	Protect	State of the art	Dynamic Threat Awareness	2 - Small to Medium	1
					3 - Medium to Large	2
					4 - Large to Super Large	2
18.3	User	Protect	State of the art	Predictive Cyber Analytics	3 - Medium to Large	2
					4 - Large to Super Large	2
18.4	All	Respond	Industry standard	Risk Response	1 - Micro to Small	5
					2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5
18.5	All	Protect	State of the art	Establish and maintain a cyber threat hunting capability	3 - Medium to Large	5
					4 - Large to Super Large	5
18.6	Strategic assets	Protect	Industry standard	Set up a risk management methodology and/or tools based on industry standards.	1 - Micro to Small	2
					2 - Small to Medium	2
					3 - Medium to Large	2
					4 - Large to Super Large	2
18.7	Strategic assets	Identify	Basic	Make key personnel aware of the main risks and how they are mitigated	1 - Micro to Small	2
					2 - Small to Medium	2
					3 - Medium to Large	2
					4 - Large to Super Large	2
18.8	Strategic assets	Identify	Industry standard	Review the risk management methodology and/or tools, periodically, taking into account changes and past incidents	1 - Micro to Small	2
					2 - Small to Medium	2
					3 - Medium to Large	2
					4 - Large to Super Large	2

Table 28: Risk Assessment and Management Control Family

5.7.19. Incident Response and Management

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
19.1	Strategic assets	N/A	Basic	Document Incident Response Policy and Procedures	1 - Micro to Small	2
					2 - Small to Medium	2

					3 - Medium to Large	2
					4 - Large to Super Large	2
19.2	Non-IT Asset	N/A	Basic	Assign Job Titles and Duties for Incident Response	3 - Medium to Large	2
					4 - Large to Super Large	2
19.3	Non-IT Asset	N/A	Basic	Designate Management Personnel to Support Incident Handling	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	2
					4 - Large to Super Large	2
19.4	Strategic assets	N/A	Basic	Devise Organization wide Standards For Reporting Incidents	3 - Medium to Large	2
					4 - Large to Super Large	2
19.5	Strategic assets	N/A	Basic	Maintain Contact Information For Reporting Security Incidents	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	2
					4 - Large to Super Large	2
19.6	Strategic assets	N/A	Basic	Publish Information Regarding Reporting Computer Anomalies and Incidents	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	2
					4 - Large to Super Large	2
19.7	N/A	N/A	Basic	Conduct Periodic Incident Scenario Sessions for Personnel	3 - Medium to Large	2
					4 - Large to Super Large	2
19.8	Strategic assets	N/A	Basic	Create Incident Scoring and Prioritization Schema	4 - Large to Super Large	2
19.9	Non-IT Asset	N/A	Basic	Alternate Communications Protocols	3 - Medium to Large	1
					4 - Large to Super Large	1
19.10	All	Protect	Industry standard	Maintainf safe mode of operation	4 - Large to Super Large	2
19.11	User	Detect	State of the art	Behavior Analysis	4 - Large to Super Large	2
19.12	All	Respond	Industry standard	Automation Support for Availability of Information and Support in Incident Response Assistance	4 - Large to Super Large	5
19.13	Strategic assets	Protect	Basic	Coordination with External Providers in Incident Response Assistance	3 - Medium to Large	1
					4 - Large to Super Large	2

Table 29: Incident Response and Management Control Family

5.7.20. Penetration Tests and Red Team Exercises

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
20.1	All	Detect	Basic	Establish a Penetration	1 - Micro to Small	3

				Testing Program	2 - Small to Medium	3
					3 - Medium to Large	4
					4 - Large to Super Large	4
20.2	All	Detect	Industry standard	Conduct Regular External and Internal Penetration Tests	3 - Medium to Large	4
					4 - Large to Super Large	4
20.3	All	Protect	Industry standard	Perform Periodic Red Team Exercises	4 - Large to Super Large	4
20.4	All	N/A	Basic	Include Tests for Presence of Unprotected System Information and Artifacts	3 - Medium to Large	1
					4 - Large to Super Large	1
20.5	All	Identify	Industry standard	Create a Test Bed for Elements Not Typically Tested in Production	3 - Medium to Large	1
					4 - Large to Super Large	2
20.6	All	Protect	Industry standard	Use Vulnerability Scanning and Penetration Testing Tools in Concert	3 - Medium to Large	2
					4 - Large to Super Large	2
20.7	Strategic assets	N/A	Basic	Ensure Results From Penetration Test Are Documented Using Open, Machine Readable Standards	4 - Large to Super Large	2
20.8	User	Protect	Basic	Control and Monitor Accounts Associated With Penetration Testing	3 - Medium to Large	5
					4 - Large to Super Large	5
20.9	All	Detect	State of the art	For Bigdata Perspective: Apply fuzzing methods for security testing	3 - Medium to Large	2
					4 - Large to Super Large	2
20.10	All	Detect	Basic	For Bigdata Perspective: Secure the system against Sybil attacks	3 - Medium to Large	5
					7 - Large to Super Large	5

Table 30: Penetration Tests and Red Team Exercises Control Family

5.7.21. Security Awareness and Training

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
21.1	User	N/A	Industry standard	Perform a Skills Gap Analysis	3 - Medium to Large	2
					4 - Large to Super Large	2
21.2	Strategic assets	N/A	Basic	Deliver Training to Fill the Skills Gap	3 - Medium to Large	2
					4 - Large to Super Large	2
21.3	N/A	N/A	Basic	Update Awareness Content Frequently	3 - Medium to Large	1
					4 - Large to Super Large	1

21.4	Strategic assets	N/A	Basic	Train Workforce on Secure Authentication	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	1
					4 - Large to Super Large	2
21.5	Strategic assets	N/A	Basic	Train Workforce on Identifying Social Engineering Attacks	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	1
					4 - Large to Super Large	2
21.6	Strategic assets	N/A	Basic	Train Workforce on Sensitive Data Handling	1 - Micro to Small	1
					2 - Small to Medium	1
					122.73 - Medium to Large	1
					4 - Large to Super Large	2
21.7	Strategic assets	N/A	Basic	Train Workforce on Causes of Unintentional Data Exposure	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	1
					4 - Large to Super Large	2
21.8	Strategic assets	N/A	Basic	Train Workforce Members on Identifying and Reporting Incidents	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	1
					4 - Large to Super Large	2
21.9	Strategic assets	N/A	Basic	Train on Insider threat	3 - Medium to Large	2
					4 - Large to Super Large	2
21.10	Strategic assets	N/A	Basic	Train and make awareness on Suspicious Communications and Anomalous System Behavior	3 - Medium to Large	2
					4 - Large to Super Large	2
21.11	Strategic assets	N/A	Basic	Conduct Role based security Traning and awareness on environmenr, security, communication, behavioural	3 - Medium to Large	2
					4 - Large to Super Large	2
21.12	Strategic assets	N/A	Basic	Simulated Events for Incident response traning	3 - Medium to Large	2
					4 - Large to Super Large	2
21.13	Strategic assets	N/A	Basic	Validate and improve awareness levels through periodic tests	2 - Small to Medium	2
					3 - Medium to Large	2
					4 - Large to Super Large	2

Table 31: Security Awareness and Training Control Family

5.7.22. External Service Management

After analyzing the number of scientific research papers and CSCD control frameworks from here, the following sub controls data are collected and mapped in different criteria.

SC No	Asset Type	CSCD Function	Sophistication Level	Sub Control (SC)	RMM Level	RL
22.1	Strategic assets	Identify	Basic	Maintain Risk Assessments and Organizational Approvals	2 - Small to Medium	1
					3 - Medium to Large	2
					4 - Large to Super Large	2
22.2	IT Hardware	Identify	Basic	Identification of Functions, Ports, Protocols, and Services	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	2
					4 - Large to Super Large	2
22.3	Strategic assets	Identify	Basic	Include security requirements and relevant tasks in contracts with third-parties and customers.	1 - Micro to Small	1
					2 - Small to Medium	1
					3 - Medium to Large	2
					4 - Large to Super Large	2
22.4	Non-IT Asset	Identify	Industry standard	Define responsibility	1 - Micro to Small	3
	Strategic assets				2 - Small to Medium	3
	User				3 - Medium to Large	4
					4 - Large to Super Large	4
22.5	Strategic assets	Identify	Basic	Set and ensure a security policy for contracts with third-parties	3 - Medium to Large	2
	Intangible assets				4 - Large to Super Large	2
22.6	Strategic assets	Identify	Basic	Review security policy for third par ties, following incidents or changes.	3 - Medium to Large	2
	Intangible assets				4 - Large to Super Large	2
22.7	All	Protect	Industry standard	Perform risk analysis before entering any outsourcing agreement	3 - Medium to Large	5
					4 - Large to Super Large	5
22.8	All	Detect	Industry standard	Keep track of security incidents related to or caused by third-parties.	1 - Micro to Small	5
					2 - Small to Medium	5
					3 - Medium to Large	5
					4 - Large to Super Large	5
22.9	Intangible assets	Identify	Basic	Periodically review and update policy for third parties and reevaluate outsourcing agreements at regular intervals, taking into account past incidents, changes, etc.	3 - Medium to Large	2
	Non-IT Asset				4 - Large to Super Large	2

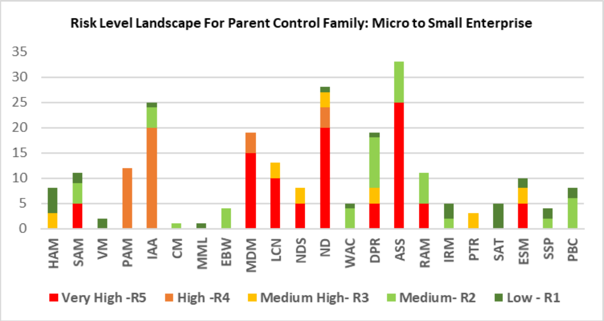
Table 32: External Service Management Control Family

5.8 Risk level Landscape based on RMM Level

Every type of RMM level enterprise has a different variation of risks. Organizations should understand the level of risks. In this part, we will illustrate the percentage of varying risk levels based on the RRM level. We used the total risk level value (R1,R2,R3,R4,R5) sum to illustrate the risk landscape of every parent control family. Then we represent the percentage of each risk level on the total sum of the risk score. For the RMM level, we have done the same calculation to find out the risk landscape and Risk percentage level.

5.8.1. Risk Level Landscape for Micro to Small Enterprise

Here we have illustrated a risk landscape for Micro to small enterprises. If we observe the left figure, we can see high-risk control family is Application Software Security (ASS), where most of the sub controls are very high R5. Besides, Network Defense Security (NDS) control has the second most very high leveled risk. The identity, Access, and Authentication (IAA) control family has a high number of R4 level sub controls. We can see more complexion of risk level illustration in right figure of a pie chart. According to the analyzed data, we have observed that about 57% of subcontrols are very risky and high risky for this type of organization. Without implementing these controls, enterprises can be at serious threat of cyber attack. Even day-to-day operation and business can be hampered significantly. For the detail of the Trigram name, Click here.



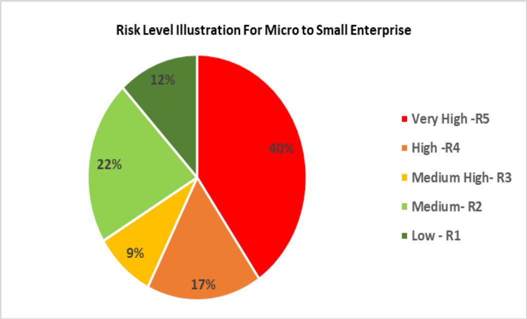
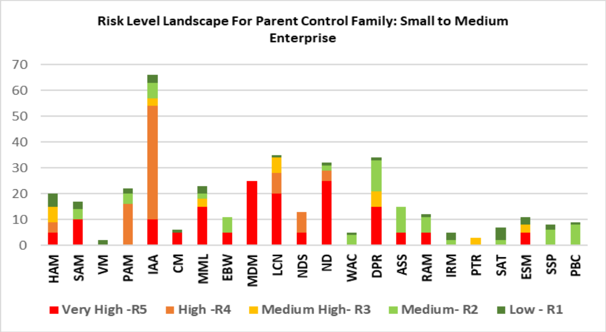


Figure 18: RL Landscape (Micro to Small), Figure 19: RL Illustration (Micro to Small)

5.8.2. Risk Level Landscape for Small to Medium Enterprise

Risk level varies for small to Medium Enterprises. Here in the left figure, we can observe a significant number of risks associated with the Identity, Access, and Authentication (IAA) control family. Sub controls of this parent control family have topmost R4 control, which gives a clear indication the necessity of enforcing these controls for cyber resilience. MML, MDM, ND, DPR control family also contains a majority number of R5 risks. On the other hand, 66% of sub controls are identified as R5 and R4 levels. That means two-third of controls are highly significant for the Small to Medium enterprise's CSCD. According to the pie chart, it shows a clear increase in risk severity of sub controls for small to medium companies than micro to small. Medium level R3 category risk exists with 17% of sub controls. For the detail of the Trigram name, Click here.



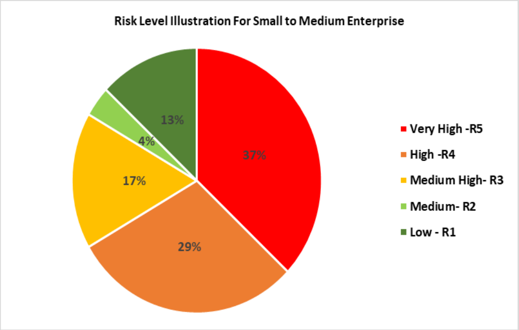
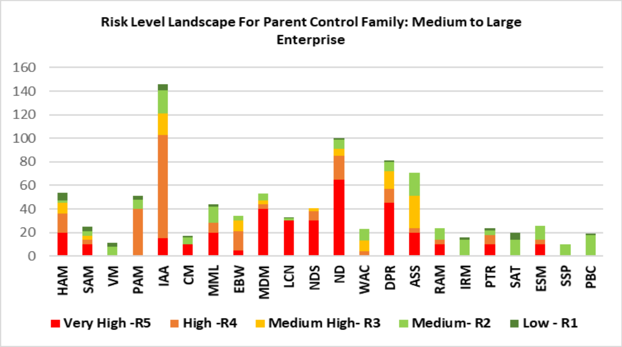


Figure 20: RL Landscape (Small to Medium),   Figure 21: RL Illustration (Small to Medium)

5.8.3. Risk Level Landscape for Medium to Large Enterprise

We have seen exciting changes for medium to large enterprise-level than previous ones. Though risk level seems to remain the same but the risk landscape provides the diversity of risk level for different parent control families. Interestingly, we observe the risk level score is high for IAA parent control, where the second most risky parent control is ND here. Having a very high R5 risk level score gives a clear indication about the severity level of subcontrols of this parent control family. Moreover, it is also observed that all parent control family contains more risk level score than previous RMM level. This is how we get the idea that medium to large enterprises has more specific controls than small to medium enterprises. Usually, this type of RMM level has more impact than lower-level enterprises. The absence of top risky controls can increase the risk of cyber-attacks and resilience. For the detail of the Trigram name, Click here.



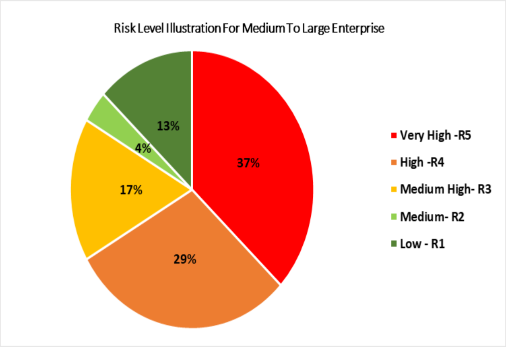
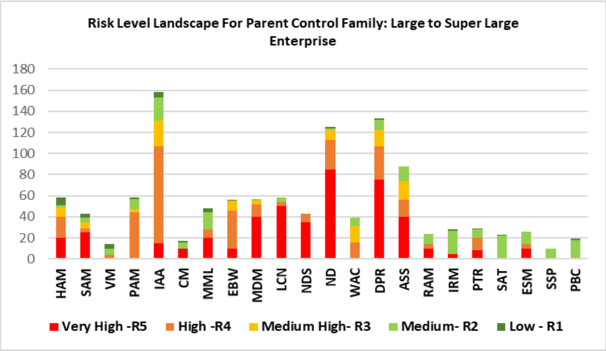


Figure 22: RL Landscape (Medium to Large), Figure 23: RL Illustration (Medium to Large)

5.8.4. Risk Level Landscape for Large to Super Large Enterprise

After analyzing data for large and Super large organizations control risk, we have got another diverse result. Here according to the second figure (Figure 6.8.3.2) 69% of sub controls are specified in R4 and R5 level, which is high in nay RMM level enterprise. Importance of the CSCD control implementation pointing the high-risk impact on cybersecurity and business continuity. The overall stability of a company can be under serious threat for just only lack of cybersecurity and cyber defense measure. However, we see IAA contains the highest risk level score where most of the controls are R4 level. The second-highest spot of parent control goes to DPR. ND contains a high number of R5 level risk controls. If we compare DPR with ND parent controls here, we see ND control has a high-risk levels (R5 and R4) here. Remarkably all parent controls contain a high-risk level score for large and super large enterprises. Maintaining operation continuation, cyber safety, and security, there is no alternative to implementing high-risk parent controls. For the detail of Trigram name, Click here



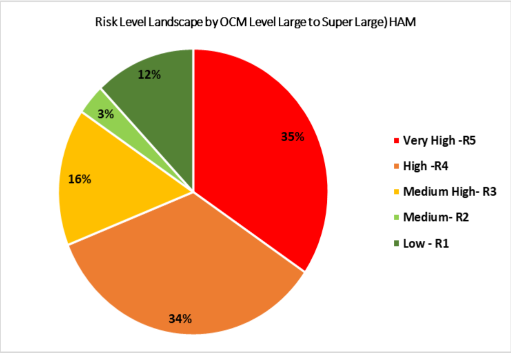


Figure 24: RL Landscape (Large to Super Large), Figure 25: RL Illustration (Large to Super Large)

5.9. Overall Risk Landscape all types of Enterprises Based on Risk Score:

In this part, the overall risk level score landscape of parent controls is illustrated based on RMM level enterprise. First of all, it is clearly indicated that IAA control family contains the most CSCD control for medium to large and Large to super large organizations. Nevertheless, we have observed a number of controls are much for ND, DPR, and ASS controls families for these RMM levels. If we look at small to medium maturity level enterprises, we see the importance of IAA still exists there with most controls. The micro to small maturity level companies' major CSCD control is ND. For the detail of the Trigram name, Click here.

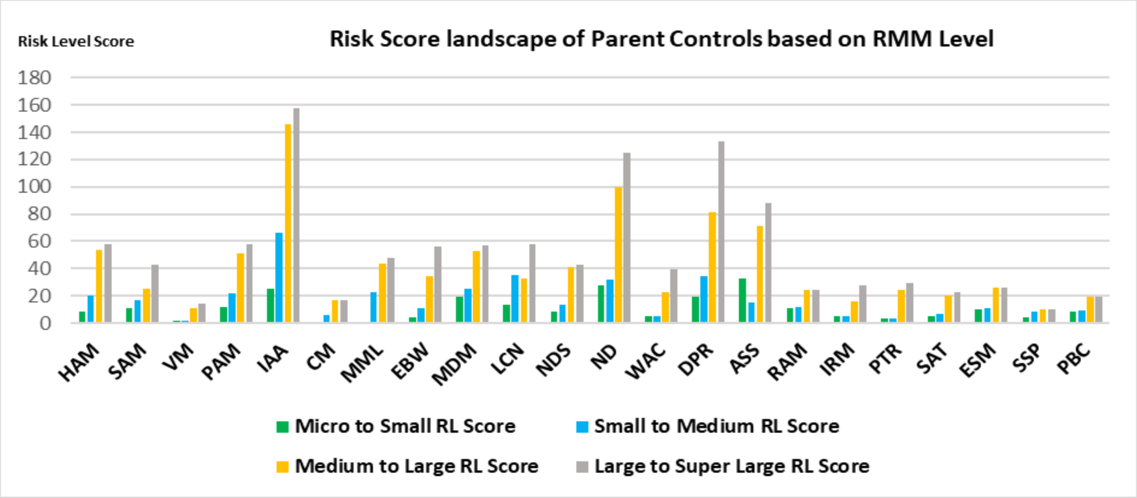


Figure 26: Risk Score Landscape of parent controls based on RMM Level

5.10. CSCD High Risk Parent Control Family landscape based on RMM Level:

After analyzing multiple aspects of risks for inactive controls, here we get overall risk score of all parent controls based on RMM level enterprises. We represent data according to high-risk control to low-risk control families. Thus, it will be easily understood about the top risky controls of a specific type of organization. We can see diverse results about top risky controls in the following table. For A-level organization's most risky control family is ASS. That means the inactivity of this control will create severe risk for that type of organization. Hence, MML controls are less risky controls in this family. On the other side, risky top control is changed in small to medium-level organizations. In this RMM category, IAA , LCN, DPR, ND, and MDM are the top five high-risk control families. VM management is considered a low priority control in this type of organization.

For the medium to large and large to super large RMM type enterprises have most of the controls. Even we have observed fluctuation of risk score there. Both RMM level organization type has same high-risk controls of IAA family but second risky control gets changed to ND in C level companies whereas DPR contains second risk level score for D level companies. In terms of risk score, we have observed less fluctuation between these two types RMM category, but for a specific control, sometimes fluctuation gets higher than A level to D level company based upon the CSCD capability. The bottom two fewer controls families remain the same in C and D level RMM enterprises.

For the detail of Trigram name, Click here

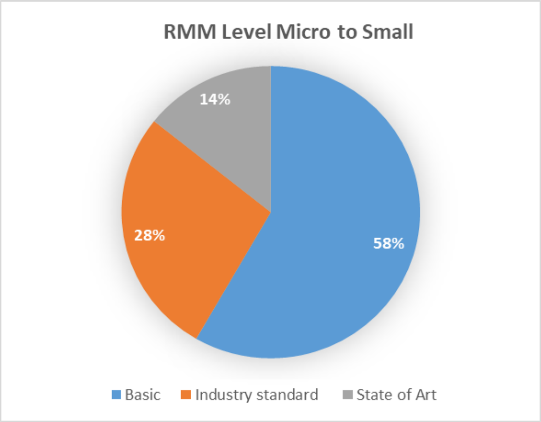
SL	Micro to Small (A)		Small to Medium (B)		Medium to Large (C)		Large to Super Large (D)	
	Tri Name	RL Score	Tri Name	RL Score	Tri Name	RL Score	Tri Name	RL Score
1	ASS	33	IAA	66	IAA	146	IAA	158
2	ND	28	LCN	35	ND	100	DPR	133
3	IAA	25	DPR	34	DPR	81	ND	125

4	MDM	19	ND	32	ASS	71	ASS	88
5	DPR	19	MDM	25	HAM	54	HAM	58
6	LCN	13	MML	23	MDM	53	PAM	58
7	PAM	12	PAM	22	PAM	51	LCN	58
8	SAM	11	HAM	20	MML	44	MDM	57
9	RAM	11	SAM	17	NDS	41	EBW	56
10	ESM	10	ASS	15	EBW	34	MML	48
11	HAM	8	NDS	13	LCN	33	SAM	43
12	NDS	8	RAM	12	ESM	26	NDS	43
13	PBC	8	EBW	11	SAM	25	WAC	39
14	WAC	5	ESM	11	RAM	24	PTR	29
15	IRM	5	PBC	9	PTR	24	IRM	28
16	SAT	5	SSP	8	WAC	23	ESM	26
17	EBW	4	SAT	7	SAT	20	RAM	24
18	SSP	4	CM	6	PBC	19	SAT	23
19	PTR	3	WAC	5	CM	17	PBC	19
20	VM	2	IRM	5	IRM	16	CM	17
21	CM	1	PTR	3	VM	11	VM	14
22	MML	1	VM	2	SSP	10	SSP	10

Figure 27: CSCD High-Risk Parent Control Family landscape based on RMM Level

5.11. Diversity of Sophistication Level on RMM Level Enterprise

We have defined CSCD sophistication level for effective implementation and practice of subcontrols. After gathering all data from our research, we have observed interesting results of changing sophistication levels for different RMM level institutions. At first, we sort down specified control family then calculate the percentage of each sophistication level. In the following illustration, we have seen the majority of sub controls (58%) are basic, 28% are Industry standard, and 14% sub controls are state of the art sophistication type for micro to small enterprises.



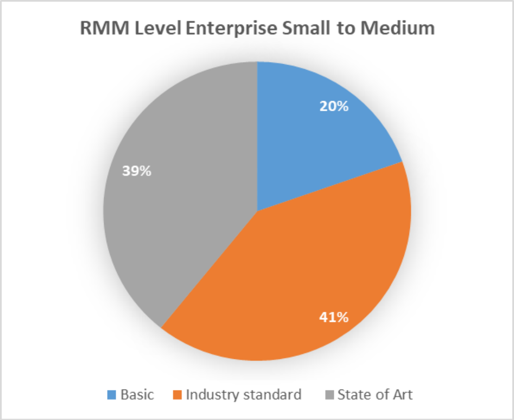
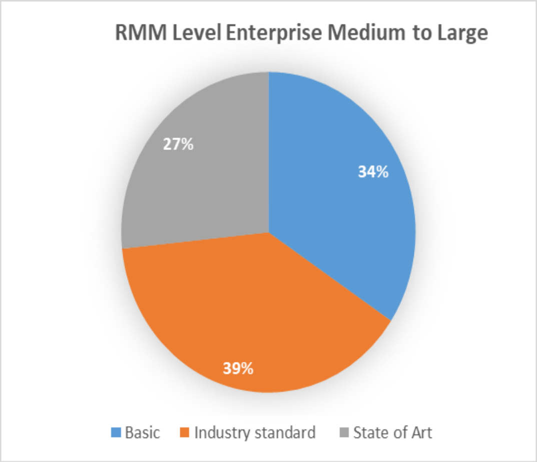


Figure 28: Sophistication level on micro to small, Figure 29: Sophistication level on Small to Medium



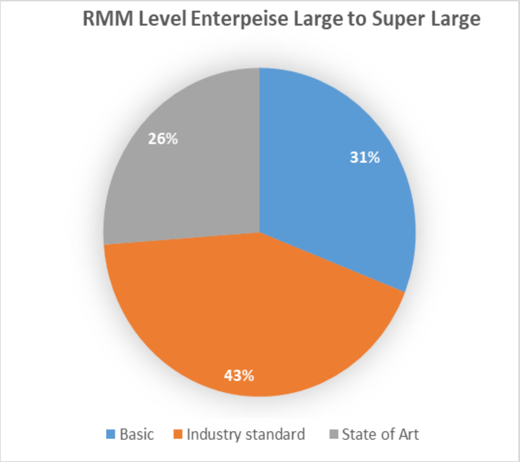


Figure 30: Sophistication level on Medium to large, Figure 31: Sophistication level on Large to Super Large

On the other hand, we have seen drastic changes in the sophistication level for small to medium level enterprises. Here 43% of controls require industry-standard implementation and support. Nevertheless, 39% of controls defined state-of-the-art sophistication level. These data give clear indication that small to medium level companies require more skillful resources to implement and manage CSCD controls. If we look on to medium to large and large to medium level organizations, it is clearly visible that the majority of controls are industry-standard, whereas 43% is the highest in D Level institutes among other RMM levels. An interesting fact is that the small to medium level companies have a majority number 39% of controls required sate of art level implementation and management.

6.0 CONCLUSION

In this section, it is important to acknowledge and mention that the objectives that were set prior to start research have been achieved by this work. Information collected from a large number of scientific papers and frameworks makes it possible to prepare a comprehensive result. There is no doubt that cybersecurity is a great matter of concern for every type of organization. By this research will contribute to define in the cybersecurity and cyber defense strategy for better planning to safeguard specific enterprises to maintain cyber resilience.

6.1 SYNTHESIS OF THE RESEARCH

Getting a solid idea about CSCD controls is important for the overall organization. This author (Byres & Hoffman, 2004) recommends some points to focus on about cybersecurity risks. In the paper author emphasis, it is first understanding the vulnerability and the approaches to secure the system. Besides, a strong recommendation was given about preparing a security policy for the IT asset. On the other hand author (Schaffner, 2019) clearly described the control criteria and category of cybersecurity. The author also suggests identifying and assess changes that significantly impact the system of internal control. Moreover, we get a clear understanding from that same research paper about the contribution of implementing and measuring control impact.

Regarding adopting a Critical and Proactive Posture on CSCD Standards, the author gives high importance on it and also narrated that there is not any universal standard to rely on for organizational CSCD (Piètre-Cambacédes et al., 2011). In addition, we also get an idea about adaptability and getting leverage from the existing framework. Therefore, enterprises need to identify critical CSCD control by control risk assessment in order to safeguard IT asset. After analysing (HM Government, 2020) Cybersecurity strategy, it is very clear that cyber threats are increasing more to large enterprises.

In order to provide secure and compliant access to IT resources, centralized identity and access management (IAM) have become one of the main challenges for companies (Kunz et al., 2019). Literature from this paper (Kruger & Mama, 2012), illustrated how important are identity management implementation and its impact to the organization's structures, policies, practices and technology platforms. According to (Fuchs & Pernul, 2007)it specifically issues such as risk management, governance, and compliance that require IdM attention within information security management. (Technology et al., 1999) contends that IdM addresses more than just security issues, providing business value through auditing, compliance, and monitoring.

The stationary nature of traditional intrusion detection systems makes them vulnerable to network instability as well as the attacks they seek to detect (Frincke & Wilhite, 2001). When considering network security, it must be emphasized that the whole network is secure (Bhavya Daya, 2013) . Network security does not only concern the security in the computers at each end of the communication chain, rather Securing the network is just as important as securing the computers and encrypting the message becasue a possible hacker can target communication chanel ,obtain data and decript it (Bhavya Daya, 2013). In a computer network basically, there are two types of attack can happen. When a network intruder intercepts data traveling through the network is known as passive network attack and when an intruder initiates commands to disrupt the network's normal operation is identified as an active attack (Pawar & Anuradha, 2015). Therefore, it makes very clear that if any network is compromised, then the impact on the company and business can be massive. That is why Network defense is considered as one of the top control for CSCD.

6.2 Limitations of the Work

It has always been crucial to identifying the limitation of work when it is based on scientific research, including with cross information technology domain aspect. Cybersecurity and cyber defense are vast fields of study. The diversity of the technology is really vast in CSCD field. Vital part of this research is to understand about the different CSCD control families from different frameworks. As because of the diverse knowledge included, understanding about the different control was the most time-consuming part of the research. In order to identify the top CSCD control family, we had to analyze large number of controls. The different framework has a different way of representation of control. Among of them to categorized all controls in a common criteria was the most difficult part. Another important thing is that we considered only renowned framework control for data reliability. In out data sampling of CSCD controls, there would be some widely used controls missing or not considered because of difficulties putting in the same categorization, specify outcome and evaluate or understand of control’s impact on RMM level enterprises.

As the research is conducted based upon survey, observation, and analysis of different frameworks, the accuracy and quality of research can be higher if more time and range of the scientific paper or framework could increase. Likewise, criteria definition can be more improved. Based on other frameworks or scientific paper analyses, the possible improvement criteria have been defined for risk scoring for control unavailability. As because there is a lack of a well-defined method for defining CSCD control risk scoring, we had to consider and use usually Cybersecurity risk assessment in our research and measuring risk for not active controls.

6.3 Next steps and Future Work

Next step and future work will be done based on the limitation mentioned above. At first, we need to focus on the CSCD control data quality and clarity. Without having quality data it would not be possible to get an accurate result. Understanding each control's absence risk is very important for the enterprises. As because each control implementation requires IT capability, budget and planning, a well-defined strategy can help enterprises to ensure cyber resilience to implement these. Moreover, understanding the sophistication level of controls are important, although according to the different level, organizations may have different expertise and complexity on sophistication. More data and information about control implementation can be collected to make more accuracy of control sophistication on RMM level enterprises.

In the same way, sector-wise, to some extend, different control implementation might have different challenges. Even the control absence risk varies to different levels of companies. Defining and implementing strategy will be easier if the idea about control absence risk is determined more accurately of the specific organizational level. To do so in the future, more accurate data can be collected about sector-wise control absence risk. A survey can be conducted to RMM level companies together with actual data.

In recent years, cyber threats and ways of attacks have been changed dramatically. With the advancement of technologies, IT systems are driven by disruptive technologies that are same under massive threat as conventional information systems. IoT, blockchane, AI, space colonization, bio-medical innovation, 3d printing, robotics, virual & augmented reality, and quantum computing are the latest field of disruption technologies. These days we have seen the uses of such technologies more widely than past. That is why explore more in disruptive technologies security in terms of CSCD context will be a great scope of future work. In this area, CSCD controls are not get matured enough as the technology is still in growth. Different technological knowledge can be gained by Identifying CSCD control data.

REFERENCES

Agency, U. D. of H. S. cyber security and I. security. (2020a). *CYBER RESILIENCE REVIEW (CRR)*.

Agency, U. D. of H. S. cyber security and I. security. (2020b). *CYBER RESILIENCE REVIEW (CRR) Method Description and Self-Assessment User Guide*.

Al-Far, A., Qusef, A., & Almajali, S. (2019). Measuring Impact Score on Confidentiality, Integrity, and Availability Using Code Metrics. *ACIT 2018 - 19th International Arab Conference on Information Technology*. https://doi.org/10.1109/ACIT.2018.8672678

Amit, R., & Schoemaker, P. J. H. (1993). Strategic assets and organizational rent. *Strategic Management Journal*, *14*(1), 33–46. https://doi.org/https://doi.org/10.1002/smj.4250140105

Arunkumar, S., Srivatsa, M., Braines, D., & Sensoy, M. (2013). Assessing trust over uncertain rules and streaming data. *Proceedings of the 16th International Conference on Information Fusion, FUSION 2013*, 922–929.

ASEC. (2020). 2017 Trust Services Criteria for Security , Availability , Processing Integrity , Con f identiality , and Privacy. In *ASEC* (Issue March).

Aspa, J. (2017). Why is Cybersecurity Important? In *Investing News Network: Vol. September* (pp. 6–8). https://investingnews.com/daily/tech-investing/cybersecurity-investing/why-is-cybersecurity-important/

Atoum, I., Otoom, A., & Ali, A. A. (2014). A holistic cyber security implementation framework. *Information Management and Computer Security*, *22*(3), 251–264. https://doi.org/10.1108/IMCS-02-2013-0014

Barrett, M. (2018). Framework for improving critical infrastructure cybersecurity. *Proceedings of the Annual ISA Analysis Division Symposium*, *535*, 9–25.

Bhavya Daya. (2013). Network security: History, importance, and future. *University of Florida Department of Electrical and …*, 13. http://www.alphawireless.co.za/wp-content/uploads/2013/01/Network-Security-article.pdf

Bodeau, D., Boyle, S., & Fabius-greene, J. (2010). Cyber Security Governance A Component of MITRE ' s Cyber Prep Methodology. *Governance An International Journal Of Policy And Administration*, *September*, 45. https://www.mitre.org/publications/technical-papers/cyber-security-governance

Bornemann, M., & Leitner, K.-H. (2002). Measuring and reporting intellectual capital: the case of a research technology organisation. *Singapore Management Review*, *24*, 7+.

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Boyens, J., Bartol, N., & Paulsen, C. (2015). NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations. *NIST Special Publication 800-161*.

Brodin, M. (2019). A Framework for GDPR Compliance for Small - and Medium - Sized Enterprises. *European Journal for Security Research*, *4*(2), 243–264. https://doi.org/10.1007/s41125-019-00042-z

Byres, E., & Hoffman, D. (2004). *006.Geruchten en feiten achter de cyberbeveiligingsrisico's van industriële controlesystemen*.

Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*(1), 1–13. https://doi.org/10.1186/s40163-020-00123-8

Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., Sweetnam, J., & Townsend, A. (2020). *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events*. 1800–1826. https://www.nccoe.nist.gov/projects/building-

Chen, K. (2018). Guideline on Effectively Managing Security Service in the Cloud. *Cloud Security Alliance*.

CIS. (2018). Internet Security ® Risk Assessment Method For Reasonable Implementation and Evaluation of CIS Controls TM. *Center for Internet Security*, *April*.

CIS. (2019). CIS Controls v7.1. *Center for Internet Security, Inc.*

CISA. (2014). *CISA Review Manual 2014_Use thesis writing.pdf*.

Commerce, U. S. D. of, & Wilbur L. Ross, Jr., S. (2020). Control Baselines for Information Systems and Organizations. *NIST Special Publication 800-53B*, *800-53B*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf

Commission, E., & Affairs, F. (2006). *M Ultinationals ' L Ocation C Hoice , and P Ublic I Ncentives*. *107*(February 2003), 81–107.

Couce-Vieira, A., Insua, D. R., & Kosgodagan, A. (2020). Assessing and forecasting cybersecurity impacts. *Decision Analysis*, *17*(4), 356–374. https://doi.org/10.1287/DECA.2020.0418

Cronin, C. (2018). *CIS RAM Express Edition Version 1.0*.

CSA. (2016). *Bigdata: Security and Privacy handbook*.

CSA. (2017). *Security Guidance for critical areas of focus in cloud computing v4.0*.

CSA. (2019). *Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure*. *December*. https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/guide_to_conducting_cybersecurity_risk_assessment_for_cii.pdf

CSA. (2020). *CSA ' s Perspective on Cloud Risk Management*.

CSA. (2021). *CSA Guide to the IoT Security Controls Framework Version 2*.

Dawson, M. (2017). *Hyper-connectivity : Intricacies of national and international cyber securities Hyper-connectivity : Intricacies of national and international cyber securities . Maurice Dawson Submitted in partial fulfillment of the award of Doctor of Philosophy by Prior*. *January*.

DCSA. (2020). *Digital Container Shipping Association*.

Dresner, D. G., Randall, J., & Philpott, E. (2018). The IASME Governance Standard for Information and Cyber Security. *IASME*, 1–46.

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship*, *8*(1). https://doi.org/10.1186/s13731-

019-0105-z

Elkhannoubi, H. (2015). *Fundamental pillars for an effective cybersecurity strategy*. 15–16.

ENISA. (2006). Cyber Insurance: Recent Advances, Good Practices and Challenges. *Computers and Security*, *24*(4), 124–133. https://dl.acm.org/citation.cfm?id=743868#.WteMrPSoxGk.mendeley%0Ahttp://dx.doi.org/10.1016/j.cose.2017.01.004%0Ahttp://dx.doi.org/10.1016/j.im.2012.08.001%0Ahttps://doi.org/10.1080/19312458.2017.1396583%0Ahttp://dx.doi.org/10.1016/j.dss.2008.11.010%0Ahtt

ENISA. (2016a). ENISA Work programme: Including multiannual planning. *Publications Office of the European Union,ENISA*. https://doi.org/10.2824/992201

ENISA. (2016b). *Technical guidelines for implementation of minimum security measures for digital service providers* (Issue December). https://doi.org/10.2824/456345

ENISA. (2017). *Cyber Security Culture in organisations* (Issue November). https://doi.org/10.2824/10543

ENISA. (2018a). *Cybersecurity Culture Guidelines : Behavioural Aspects of Cybersecurity* (Issue December). https://doi.org/10.2824/324042

ENISA. (2018b). *Economics of vulnerability disclosure* (Issue December). https://doi.org/10.2824/49807

Escalante, R., & Maier-Speredelozzi, V. (2008). Selecting facility locations and transportation for multinational corporation supply chains. *IIE Annual Conference and Expo 2008*, 1629–1634.

ETSI. (2015a). Critical Security Controls for Effective Cyber Defence. In *ETSI* (Vol. 1).

ETSI. (2015b). *Critical Security Controls for Effective Cyber Defence* (Vol. 1).

ETSI. (2016a). *Critical Security Controls for Effective Cyber Defence ; Part 2 : Measurement and auditing* (Vol. 1).

ETSI. (2016b). *Critical Security Controls for Effective Cyber Defence ; Part 3 : Service Sector Implementations* (Vol. 1).

ETSI. (2016c). *Critical Security Controls for Effective Cyber Defence ; Part 4 : Facilitation Mechanisms* (Vol. 1).

ETSI. (2018a). *Critical Security Controls for Effective Cyber Defence ; Part 1 : The Critical Security Controls* (Vol. 1).

ETSI. (2018b). *Critical Security Controls for Effective Cyber Defence ; Part 5 : Privacy enhancement* (Vol. 1).

ETSI. (2018c). Security techniques for protecting software. In *ETSI* (Vol. 1).

ETSI. (2020). Cyber Security for Consumer Internet of Things. *ETSI*, *1*, 1–34.

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, *9*(17), 4667–4679. https://doi.org/10.1002/sec.1657

Fedramp. (2018). *FedRAMP Continuous Monitoring Performance Management Guide*.

FEDRAMP. (2017a). *FedRAMP CONTROL SPECIFIC CONTRACT*.

FEDRAMP. (2017b). *FedRAMP SECURITY ASSESSMENT*.

FEDRAMP. (2018). *Automated Vulnerability Risk Adjustment Framework*.

FEDRAMP. (2020). *Agency Guide for Continuous Monitoring*.

FISMA. (2020). *FISMA Audit*. https://oig.federalreserve.gov/fisma.htm

Foss, N., & Knudsen, T. (2003). The Ressource-Based Tangle: Towards a Sustainable Explanation of Competitive Advantage. *Managerial and Decision Economics*, *24*, 291–307. https://doi.org/10.1002/mde.1122

Frey, B. B. (2018). *The SAGE Encyclopedia of Educational Research, Measurement, and Evaluation*. https://doi.org/10.4135/9781506326139 NV - 4

Frincke, D., & Wilhite, E. (2001). Distributed Network Defense. *Information Systems Security*, 5–6.

Fuchs, L., & Pernul, G. (2007). Supporting compliant and secure user handling - A structured approach for in-house identity management. In *Proceedings - Second International Conference on Availability, Reliability and Security, ARES 2007* (pp. 374–381). https://doi.org/10.1109/ARES.2007.145

Galbreath, J. (2005). Which resources matter the most to firm success? An exploratory study of resource-based theory. *Technovation*, *25*(9), 979–987. https://doi.org/10.1016/j.technovation.2004.02.008

Galinec, D., Moznik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika*, *58*(3), 273–286. https://doi.org/10.1080/00051144.2017.1407022

Galligan, M. E., & Rau, K. (2015). COSO in the cyber age. In *Deloitte*.

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Analysis*, *40*(1), 183–199. https://doi.org/10.1111/risa.12891

Gashgari, G., Walters, R., & Wills, G. (2017). A proposed best-practice framework for information security governance. *IoTBDS 2017 - Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security*, *IoTBDS*, 295–301. https://doi.org/10.5220/0006303102950301

GDPR EU. (2018). *GDPR Checklist* (Issue May). https://gdpr.eu/checklist/

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, *34*(5), 509–519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001

Hammer, J. H., & Schneider, G. (2007). On the definition and policies of confidentiality. *Proceedings - IAS 2007 3rd Internationl Symposium on Information Assurance and Security*, 337–342. https://doi.org/10.1109/IAS.2007.20

Henriques de Gusmão, A. P., Mendonça Silva, M., Poleto, T., Camara e Silva, L., & Cabral Seixas Costa, A. P. (2018). Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. *International Journal of Information Management*, *43*(January), 248–260. https://doi.org/10.1016/j.ijinfomgt.2018.08.008

Hipaa. (2020). *HIPAA COMPLIANCE*.

Hitrust CSF. (2020). *HITRUST Framwork* (Issue December).

HM Government. (2020). *National Cyber Security Strategy - Progress Report*. 43. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Hutchins, E., Cloppert, M., & Amin, R. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *6th International Conference on Information Warfare and Security, ICIW 2011*, *July 2005*, 113–125.

Integration, E. E. (2007). Different . Types . of . Business-. In *Group*.

International Telecommunication Union. (2008). Overview Cybersecurity. *ITU-T X.1205 Recommendation*, *1205*(Rec. ITU-T X.1205 (04/2008)), 2–3. https://www.itu.int/rec/T-REC-X.1205-200804-I

ISO/IEC. (2013). ISO/IEC 27002:2013.pdf. *Iec*, *2013*, 90. www.iso.org

ISO. (1987). Information technology - IT asset management. In *ISO/IEC 19770-1* (Vol. 1987).

ISO. (2013). Information technology - Security techniques - Information security management systems - Requirements. *ISO 27001*.

ISO. (2017). ISO_IEC 19770-1_2017(en), Information technology — IT asset management — Part 1_ IT asset management systems — Requirements. *ISO IEC 19770-1*. https://www.iso.org/obp/ui/#iso:std:iso-iec:19770:-1:ed-3:v1:en

ISO IEC. (2013). *INTERNATIONAL STANDARD ISO 27002 / IEC Information technology — Security techniques — Code of practice for information security controls*. *2013*.

James, L. (2018). Making cyber-security a strategic business priority. *Network Security*, *2018*(5), 6–8. https://doi.org/10.1016/S1353-4858(18)30042-4

Jennex, M. E., & Zyngier, S. (2007). Security as a contributor to knowledge management success. *Information Systems Frontiers*, *9*(5), 493–504. https://doi.org/10.1007/s10796-007-9053-4

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126–129. https://doi.org/10.1145/1435417.1435446

Karen Scarfone, Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical Guide to Information Security Testing and Assessment Special Publication 800-115. *Nist Special Publication*, *800*, 1–80. http://books.google.com/books?hl=en&lr=&id=EHrf6q7GobUC&oi=fnd&pg=PR7&dq=Technical+Guide+to+Information+Security+Testing+and+Assessment+Recommendations+of+the+National+Institute+of+Standards+and+Technology&ots=FTcnroLXL8&sig=DE

Kay, J. (2003). Foundations of Corporate Success. *Foundations of Corporate Success*, 1–11. https://doi.org/10.1093/019828988x.001.0001

Kelley, D. (2014). *NIST Risk Management Framework Summery*. 1–43.

Kiesling, T., Niederl, J., Ziegler, J., & Krempel, M. (2016). A model-based approach for aviation cyber security risk assessment. *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, 517–525. https://doi.org/10.1109/ARES.2016.63

King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. *Frontiers in Psychology*, *9*(FEB), 1–19. https://doi.org/10.3389/fpsyg.2018.00039

Kolini, F., & Janczewski, L. (2015). *Cyber Defense Capability Model: A Foundation Taxonomy*. http://aisel.aisnet.org/confirm2015%0Ahttp://aisel.aisnet.org/confirm2015/32%0Ahttp://aisel.aisnet.org/cgi/viewcontent.cgi?article=1015&context=confirm2015%0Ahttps://doc-00-14-docs.googleusercontent.com/docs/securesc/4hihe8uk61otv6kdo3cmc2725ckc7be6/p3ice

KPMG. (2019). *Cyber Maturity Assessment - KPMG Global*. https://home.kpmg/au/en/home/services/advisory/management-consulting/technology/cyber-security/cyber-strategy-governance/cyber-maturity-assessment.html

Kruger, C. J., & Mama, M. N. (2012). Incorporating business strategy formulation with identity management strategy formulation. *Information Management & Computer Security*, *20*(3), 152–169. https://doi.org/10.1108/09685221211247271

Kumar, R. (2015). The Problem of Attribution in Cyber Security. *International Journal of Computer Applications*, *131*(7), 34–36. https://doi.org/10.5120/ijca2015907386

Kunz, M., Puchta, A., Groll, S., Fuchs, L., & Pernul, G. (2019). Attribute quality management for dynamic identity and access management. *Journal of Information Security and Applications*, *44*, 64–79. https://doi.org/10.1016/j.jisa.2018.11.004

Kyengo, J. M., & Kilika, J. (2017). Strategic Assets, Competitive Capabilities and Firm Performance: Review of the Literature. *Journal of Business and Economic Development*, *2*(3), 140–147. https://doi.org/10.11648/j.jbed.20170203.11

Lanter, D. (2019). COBIT 2019 Framework Introduction and methodology. *ISACA*, 2–64. https://community.mis.temple.edu/mis5203sec001sp2019/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf

Lopez, V. (2001). *Overview of ResourceAn overview review of the resource-based view (RBV) of the firm, drawing on recent Spanish management research*. Irish Journal of Management; Dublin Vol. 22, Iss. 2,.

Lse, C. T., Andrew, C., & Bernard, B. (2019). *Multinational Firms' Market Entry and Expansion, with Evidence from Eastern Europe*.

Majhi, S. K., & Dhal, S. K. (2016). A Study on Security Vulnerability on Cloud Platforms. *Physics Procedia*, *78*(December 2015), 55–60. https://doi.org/10.1016/j.procs.2016.02.010

Mavroeidis, V., & Bromander, S. (2017). Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. *Proceedings - 2017 European Intelligence and Security Informatics Conference, EISIC 2017*, *2017-Janua*, 91–98. https://doi.org/10.1109/EISIC.2017.20

McAfee. (2020). How Cybersecurity Policies and Procedures Protect Against Cyberattacks. In *McAfee*. https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/cybersecurity-policies.html

NCES. (1998). *Safeguarding Your Technology*. NCES Publication 98-297 (National Center for Education Statistics). https://nces.ed.gov/pubs98/safetech/chapter5.asp

Nieles, M., & Dempsey, K. (2017). An Introduction to Information Security An Introduction to Information Security. *NIST Special Publication - 800 Series*.

NIST. (2011). Managing Information Security Risk. *NIST Special Publication 800-39*, *40*(March), 5–9. https://doi.org/10.1108/k.2011.06740caa.012

NIST. (2018). SP NIST 800-037, Rev.2, Risk Management Framework (RMF) for Information Systems and Organizations. *NIST Special Publication - 800 Series*, 183. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final%0Ahttps://doi.org/10.6028/NIST.SP.800-37r2

NIST CSRC. (2021). *data asset - Glossary CSRC*. https://csrc.nist.gov/glossary/term/data_asset#:~:text=A data asset also includes,would be a data asset.

Obama, B. (2013). Executive Order -Improving Critical Infrastructure Cybersecurity - February 12, 2013. *Whitehouse.Gov*, 1. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Ostrom, E. (2011). *Background on the Institutional Analysis and*. *39*(1), 7–27.

Patel, S. C., Graham, J. H., & Ralston, P. A. S. (2008). Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. *International Journal of Information Management*, *28*(6), 483–491. https://doi.org/10.1016/j.ijinfomgt.2008.01.009

Pawar, M. V., & Anuradha, J. (2015). Network security and types of attacks in network. *Procedia Computer Science*, *48*(C), 503–506. https://doi.org/10.1016/j.procs.2015.04.126

PCIDSS. (2018). Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures. In *PCI Security Standards Council* (Issue May).

Pernice, I. (2018). Global cybersecurity governance: A constitutionalist analysis. In *Global Constitutionalism* (Vol. 7, Issue 1, pp. 112–141). https://doi.org/10.1017/S2045381718000023

Piètre-Cambacédes, L., Tritschler, M., & Ericsson, G. N. (2011). Cybersecurity myths on power control systems: 21 misconceptions and false beliefs. *IEEE Transactions on Power Delivery*, *26*(1), 161–172. https://doi.org/10.1109/TPWRD.2010.2061872

Poore, R. S. (2006). Information security governance. *Information Security Management Handbook, Fifth Edition*, *3*(April), 179–188. https://doi.org/10.1201/9781439833032.ch8

Proctor, R. W., & Chen, J. (2015). The Role of Human Factors/Ergonomics in the Science of Security: Decision Making and Action Selection in Cyberspace. *Human Factors*, *57*(5), 721–727. https://doi.org/10.1177/0018720815585906

Rebecca M. Blank. Patrick D. Gallagher. (2012). NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments. *NIST Special Publication*, *September*, 95.

Ritchey, D. (2019). Critical Infrastructure Security and Resilience -- Today and Tomorrow. In *Security: Solutions for Enterprise Security Leaders*. https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=138853858&site=eds-live

Röcher, D.-J. (2018). Cyber Threat Intelligence 101. *Datenschutz Und Datensicherheit - DuD*, *42*(10), 623–628. https://doi.org/10.1007/s11623-018-1013-2

Rosenzweig, P. (2013). *International Law and Private Actor Active Cyber Defensive Measures*. 1–13. https://doi.org/http://dx.doi.org/10.2139/ssrn.2270673

Roure, D., Nurse, R. C., & Montalvo, M. (2019). *Munich Personal RePEc Archive Cyber Security Framework for the Internet-of-Things in Industry 4 . 0*. *92565*, 0–7. https://doi.org/10.20944/preprints201903.0111.v1

Roy, M. (2016). What is IT strategic plan (information technology strategic plan)? In *Definition from WhatIs.com*. https://searchcio.techtarget.com/definition/IT-strategic-plan-information-technology-strategic-plan

Schaffner, L. G. (2019). Cybersecurity Description and Control Criteria to Strengthen Corporate Governance. *Journal of Leadership, Accountability and Ethics*, *16*(1). https://doi.org/10.33423/jlae.v16i1.1366

Schram, A. B. (2014). A Mixed Methods Content Analysis of the Research Literature in Science Education. *International Journal of Science Education*, *36*(15), 2619–2638. https://doi.org/10.1080/09500693.2014.908328

Silva, W. N., Vaz, M. A., & Moreira Casa de Oswaldo Cruz, J. (2018). *Strategic Planning for Information Technology*. 370–385. https://doi.org/10.4018/978-1-5225-7214-5.ch016

Spiller, K. (2020). “Putting Everything up There”: Framing How We Navigate the Intricacies of Privacy and Security on Social Media. *Humanity & Society*, *45*(1), 016059762090450. https://doi.org/10.1177/0160597620904502

Spremić, M., & Šimunic, A. (2018). Cyber security challenges in digital economy. *Lecture Notes in Engineering and Computer Science*, *2235*, 2–7.

Stiawan, D., Idris, M. Y., Abdullah, A. H., Aljaber, F., & Budiarto, R. (2017). Cyber-attack penetration test and vulnerability analysis. *International Journal of Online Engineering*, *13*(1), 125–132. https://doi.org/10.3991/ijoe.v13i01.6407

Stouffer, K., Stouffer, K., Pease, M., & Mccarthy, J. (2020). Cybersecurity Framework Version 1 . 1 Manufacturing Profile Cybersecurity Framework Version 1 . 1 Manufacturing Profile. *NIST*. https://doi.org/https://doi.org/10.6028/NIST.IR.8183r1

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). Contingency Planning Guide for Federal Information Systems. *NIST Special Publication 800-34 Rev. 1*, *May*, 150.

Technology, I., Technikon, P. E., & Elizabeth, P. (1999). *Information security management: why standards are important*. 50–57.

Thayer, J. T., Burstein, M., Goldman, R. P., Kuter, U., Robertson, P., & Laddaga, R. (2013). Comparing strategic and tactical responses to cyber threats. *Proceedings - IEEE 7th International Conference on Self-Adaptation and Self-Organizing Systems Workshops, SASOW 2013*, 35–40. https://doi.org/10.1109/SASOW.2013.25

The Council of the European Union. (2013). The indentification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699.

Unal, B. (2019). Cybersecurity of NATO’s Space-based Strategic Assets. *Chatham House*, *July*. https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf

US Department of Homeland Security. (2014). *Department of Homeland Security Cybersecurity Capability Maturity Model White Paper*.

Von Solms, B. (2001). Information security - A multidimensional discipline. *Computers and Security*, *20*(6), 504–508. https://doi.org/10.1016/S0167-4048(01)00608-3

Winograd, T., Scarfone, K., Winograd, T., & Scarfone, K. (2007). Guide to Secure Web Services Recommendations of the National Institute of Standards and Technology Anoop Singhal. *NIST Special Publication - 800 Series*, *95*.

Wu, M. (2019). 10 Considerations for Cybersecurity Risk Management. In *Securityscorecard*. https://securityscorecard.com/blog/10-considerations-for-cybersecurity-risk-management

Zager, R., & Zager, J. (2018). OODA Loops in Cyberspace: a New Cyber-Defense Model. *Small Wars Journal*, *October*, 1–12. http://smallwarsjournal.com/jrnl/art/ooda-loops-cyberspace-new-cyber-defense-model

Annexes

We have conducted a risk analysis based on the gathered data. We have used Microsoft Excel to collect, analyze and model the data for the result. Detail analyses and data are given below in the attached excel.

CSCD Control
Framwork v.1.0_July