
# Operational Management
## MGMT 322

CONTENTS

# Implementing Lean design in Cyber Security Framework


Akeel Ather Medina
*DSSE Habib University*
Karachi, Pakistan
am05427@st.habib.edu.pk

Omer Rastgar
*DSSE Habib University*
Karachi, Pakistan
or05554@st.habib.edu.pk

Samarah Asghar Sahto
*DSSE Habib University*
Karachi, Pakistan
ss05563@st.habib.edu.pk

Zain Ul Haq
*DSSE Habib University*
Karachi, Pakistan
zh05616@st.habib.edu.pk


## I. Theoretical Description


***Abstract*—In this paper, we propose a novel framework for lean Cyber Security that combines the Toyota Process system, a lean framework, with the NIST Cybersecurity Framework (NIST CSF) to optimize resource utilization and improve the value chain and value of cyber security efforts. Our approach leverages the waste management methods of lean with the five functions of the NIST CSF: identify, protect, detect, respond, and recover.**

**The paper consists of two main parts: a literature review and a description of the process for developing the proposed framework. While there is literature available on both lean frameworks and cyber security frameworks, there is limited research on merging the two. Most existing Lean cyber security frameworks focus on specific systems or attacks rather than providing a generic framework for cost-effective risk management.**



***Keywords*—** NIST; TPS; LEAN; Kiazen; Cyber Security; Waste

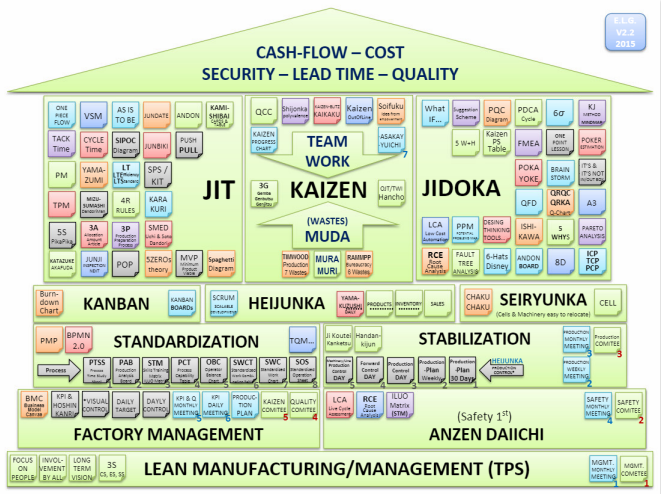




Fig. 1. Toyota Process System

## II. Introduction

he threat of cyber attacks has continued to increase, affecting both large and small businesses. While it is important to have secure systems, the focus should also be on how quickly the company can recover from an attack. A lean approach can help identify waste and generate value, while ensuring the security of assets. In 2022, the average cost of a data breach was $4.5 million globally, and it is estimated that business losses will reach approximately $10.5 trillion by 2025 [Fox, 2023]. Additional requirements like governance, risk, and compliance (GRC) can increase the loss of capital, with fines for GDPR noncompliance reaching $100 million in the first half of 2022 [Fox, 2023]. Combining a lean and cyber security framework (CFS) can generate value by keeping assets secure and reducing unnecessary waste.
Now before we go into identifying lean in CFS, we need to define the main two frameworks involved. The first one is the Toyota processing system (TPS) and the second is the national institute of standards and technology (NIST) CSF.

Toyota's production system philosophy reflects a manufacturing culture of continuous improvement centered on creating standards aimed at minimizing waste through employee engagement. The system's purpose is to shorten the time it takes from the moment an order is received. Until it is delivered to the actual consumer. Ideally, the system aims to deliver the greatest possible quality at the lowest possible cost and with the shortest feasible lead time. The figure below outline the TPS framework

The NIST framework is among the most comprehensive disaster and recovery planning frameworks, including suggestions not just on recovery planning, improvements, and communications, but also on early identification, protection, detection, and response. It was developed for US critical infrastructure and a law was passed under Section 8(c) of the Cyber Security Research and Development Act (15 U.S.C. 7406(c)). To utilize the various standards in cyber security to develop a customizable framework that can be applied to all levels of companies. Lastly, it is important to mention that NIST CSF doesn't inform how to protect a system but rather what to protect. This means that we will be using standards like ISO to implement security while using NIST as the identifier for all the possible domains where we can use it. Within the framework, NIST provides a section for informative references. These are all some of the main standards being used for that specific category. While we can also define lean in terms of specific technology, we will only focus on the higher abstraction similar to NIST CSF which uses functions such as identify, protect, detect, respond and recover.

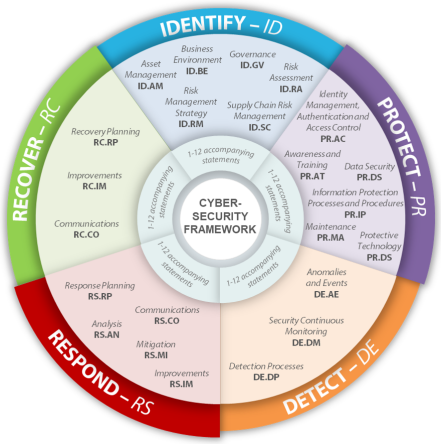



Fig. 2. Function CFS

## III. Literature Review - Assignment 2

The paper "Lean in Information Technology: Produce the Human Before the Software" examines the application of lean manufacturing and lean services principles to the development and administration of information technology goods and services. The Lean Information Technology approach attempts to create an information system that delivers the appropriate information to the appropriate people at the appropriate time and on the first attempt. In addition to emphasizing Lean IT's focus on project management institutions where planning ahead is challenging, the paper intends to demonstrate how complimentary Lean IT is to other project management methodologies like Scrum. The Lean IT approach attempts to accomplish ongoing improvement, promote teamwork, cut out non-value-added tasks, and lessen system complexity. The usage of all lean manufacturing tools, including the Japanese 5S (Structurize, Systemize, Standardize, Self-Discipline, and Sanitize) and others, is part of the Lean IT approach. The authors of the paper go on to list repetitive activity, unstable processes, low customer relationship management, and noncompliance with cost/quality/time promises as information system waste. Inadequate IT-production communication hinders service and system development while the delivery of underutilized features, poor specification of client demands, and faster or bigger quantity than the customer requested result in earlier production or too high a service level. Waste also comes from low knowledge capitalization, non-reuse of components (codes), and poor tools and skills management. Activities that do not add value to customers, such as presenting technical dashboards to managers, and unnecessary movements, such as emergency response to recurring problems, frequent change of environments (technical bases, framework, tools...), multi-staffing without prioritization, and multiple interventions on incidents without resolution, are also waste in the information system.

In addition, the authors argue that eliminating waste in the information system can be achieved by using Lean techniques. Failure Modes, Effects, and Criticality Analysis (FMECA) is a technique that can be used to prevent failures caused by unstable processes, for instance. Capitalization tools and processes, the establishment of sharing moments between teams and the customer, and the usage of collaboration platforms such as wikis and collaborative workspaces can aid in capitalizing knowledge and process reviews by identifying and eliminating non-value-added tasks. In addition, the study underlines how strategies such as the Japanese 5S principle and others can aid firms in reducing the sources of waste (Muda) in their information systems. The paper then presents the concept of utilizing IT governance tools to apply Lean Management concepts. The adapted information system was changed utilizing agile development approaches, which offer flexible organizational structures, high technical quality, repeatable automated testing, incremental designs, and collaborative work. IT Infrastructure Library (ITIL) is a conceptual framework that supports tight collaboration throughout the development cycle, but it has downsides since it is reactive and lacks insight into enhancing productivity or solving the leadership issues associated with organizational change. The Capability Maturity Model Integration (CMMI) paradigm does not address wasteful behaviors, such as poor alignment between business units and the IT function or overly complex architectural design within a software development. Consumers, suppliers, and employees can all utilize the Value Stream, which deconstructs services into their constituent process steps. The deployment of Lean management in a corporation can be related to the development of information systems that facilitate the management of software delivery schedules and significantly reduce issue reaction times. Value stream mapping, Kanban, collaborative visualization, Key Performance Indicators (KPIs), and Heijunka are a few of the techniques used by lean thinking to manage work and get rid of non-value-adding activities and unsatisfactory customer service. The paper highlights how Lean and the information system work together to create two values: one for the customer by making it easier for them to access and use the Information System, and another for the employees by making it easier for them to process and access information, freeing up their time to engage in activities that add real value. Finally, the authors also cover the difficulties in applying Lean IT principles, which are different from Lean production because IT value streams are digital and intangible. It can be challenging to visualize and quantify these processes, and cultural change may encounter resistance, especially from computer scientists who place more value on technical expertise than on the integration of their profession with skill development. Lean thinking implementation may also encounter difficulties like interpersonal conflicts, reluctance to change, and complexity brought on by changing client expectations and iterative development. [Belkadi et al., 2019]

in the paper, "Lean Production and information technology: Connection or contradiction? - ScienceDirect", Jan Riezebos investigates the relationship between lean production and information technology (IT) in manufacturing organizations in his paper, "Lean Production and information technology: Connection or contradiction?". The paper identifies that while there are areas of connection between lean production and IT, there is also a contradiction between the two approaches.

The paper argues that lean production emphasizes simplicity, standardization, and visual control, while IT is often associated with complexity, customization, and automation. Riezebos cites examples of this contradiction, such as the use of computer-aided production management software, which can lead to over-complication of product designs that are difficult to manufacture using lean principles. Additionally, IT systems that focus on automation can undermine the importance of human workers and the visual control they provide in the production process. However, the paper also identifies areas of connection between lean production and IT. For example, IT can be used to support visual management, improve communication, and facilitate problem-solving. Riezebos gives examples of how IT can facilitate visual management through the use of electronic displays that provide real-time information about production processes. IT can also improve communication by providing workers with access to information about their work and the work of others. The paper concludes that while there are challenges to integrating IT into lean production, it is possible to do so successfully with careful planning, clear objectives, and a focus on continuous improvement. Riezebos emphasizes the importance of understanding the strengths and limitations of both lean production and IT and developing a plan that leverages the strengths of both approaches while minimizing their weaknesses. [Riezebos et al., 2009]

The "Role of Information Technology in Lean Enterprise Systems" by Dubbaka and Dadkhah investigates the role of information technology (IT) in supporting lean enterprise systems. The paper argues that

the integration of IT into lean enterprise systems can improve the efficiency and effectiveness of these systems, leading to improved organizational performance. The authors begin by defining lean enterprise systems as a set of principles and practices aimed at eliminating waste and maximizing value for customers. They argue that IT can play a critical role in supporting these principles and practices by providing real-time information, facilitating communication and collaboration, and enabling continuous improvement.
The paper identifies several areas where IT can support lean enterprise systems. First, IT can be used to provide real-time information about production processes, allowing workers to identify and respond to issues as they arise. The authors give examples of how this can be achieved through the use of sensors and other monitoring technologies that collect data about production processes. Second, IT can facilitate communication and collaboration between workers, departments, and even organizations. The paper suggests that IT can enable the creation of virtual teams, allowing workers to collaborate on projects regardless of their physical location. Additionally, IT can facilitate the sharing of information and best practices between organizations, leading to improved performance across the supply chain.
Finally, the paper argues that IT can enable continuous improvement in lean enterprise systems by providing tools for data analysis and process optimization. The authors suggest that IT can be used to identify patterns in production processes, allowing organizations to make data-driven decisions about process improvement. The authors conclude that the integration of IT into lean enterprise systems can lead to significant improvements in organizational performance. However, they also acknowledge that there are challenges to integrating IT into lean enterprise systems, including issues related to data security, system complexity, and resistance to change. The authors suggest that these challenges can be overcome through careful planning, clear communication, and a focus on continuous improvement. It is especially relevant to plan for issues in data security, where implementing international standards is a safety requirement. [Dubbaka and Dadkhah, ]

The article “Poka-Yoke – Japanese for cybersecurity professionals” discusses the concept of Poka-Yoke, within the scope of cybersecurity. Shigeo Shingo, a Japanese expert in quality control systems and production processes who became famous for developing the Toyota Production System, introduced the concept of Poka-Yoke. Poka-Yoke means ”prevention of unexpected errors” and is founded on the principle of zero quality control, in which production processes are designed and arranged to prevent errors. Fail-safe and fail-secure are additional concepts established alongside Poka-Yoke, which are employed in cybersecurity as well. However, it is impossible to protect IT systems in a way that prevents breaches, and breaches will occur inevitably. Thus, the emphasis has switched to safe-to-fail, which attempts to mitigate the impact of breaches to the greatest extent possible.
According to the EY Global Information Security Study 2016-2017, cybersecurity investments are now primarily focused on prevention, segmentation, and resilience. With cyber threat intelligence and management, prevention entails recognizing a breach before it occurs. On the other hand, segmentation tries to confine the impact of a breach to one compartment of the IT system without affecting other portions. While resilience entails responding to a security breach, handling the crisis, securing evidence for court, communicating with the market, and resuming normal operations. Although Poka-Yoke has not yet been used in cybersecurity, the paper claims that this field is a promising one for its potential use. The article highlights the need to maintain a safe-to-fail strategy while balancing investments in cybersecurity across resist, sense, and react, which many firms typically lack. [Kessel, ]

In the paper, the author discusses the application of Six Sigma in Information Technology (IT) projects. Six Sigma is a data-driven approach to quality management that aims to reduce defects and variations in business processes. The author argues that Six Sigma can be effectively applied to IT projects to improve their quality, reduce costs, and increase customer satisfaction.
The paper provides an overview of the key concepts of Six Sigma and how they can be applied to IT projects. The author also shares examples of successful Six Sigma implementation in IT projects, including software development, hardware implementation, and IT service delivery.
The author suggests that Six Sigma can be a valuable tool for IT project management and can contribute to improving project outcomes. However, the paper also notes that successful implementation requires strong leadership, stakeholder engagement, and a culture of continuous improvement. Overall, the paper provides insights into how Six Sigma can be leveraged in IT projects to achieve better results.
There are examples of successful Six Sigma implementation in IT projects. For instance, the author describes a case study where Six Sigma was applied to software development processes.
The organization had been experiencing issues with software defects and customer complaints, resulting in low customer satisfaction ratings. Using the DMAIC (Define, Measure, Analyze, Improve, and Control) methodology of Six Sigma, the organization identified the root causes of the defects and implemented corrective actions to address them.
The implementation of Six Sigma led to a significant improvement in software quality, as measured by a reduction in defects and customer complaints. As a result, customer satisfaction ratings increased, and the organization was able to deliver software products more efficiently and at a lower cost.
This case study illustrates how Six Sigma can be applied to IT projects, specifically in software development processes, to achieve better outcomes. The use of Six Sigma enabled the organization to identify and address the root causes of defects, resulting in higher quality products and increased customer satisfaction. [Hsieh et al., 2007]
In the paper ”Kanban in Software Engineering: A Systematic Mapping Study” published in November 2017, the current state of knowledge on the use of Kanban in software engineering, is explored. The study utilizes a systematic mapping methodology to examine 119 primary studies on the topic. The results of the study indicate that Kanban is predominantly used in software development and maintenance, with a particular focus on process improvement, quality improvement, and productivity enhancement. The research also indicates that Kanban is effective in improving workflow, reducing cycle time, and increasing customer satisfaction. However, the study notes that there is a lack of empirical evidence on the effectiveness of Kanban in software engineering, and calls for further research in this area. Nonetheless, the research findings suggest that Kanban is a valuable tool in software engineering, and its implementation can lead to significant improvements in project outcomes. [Ahmad et al., 2018]
In the paper, ”Frameworks proposed to address the threat of cyber-physical attacks to lean 4.0 systems”, it explores the application of Lean and Six Sigma frameworks in the context of cybersecurity for Industrial 4.0 systems. Three technical frameworks for implementing cybersecurity with Lean have been proposed, but this paper focuses on designing a Cybersecurity Framework (CSF) using Lean Design to outline the cybersecurity functions in which Lean can be implemented. The authors of the proposed frameworks focus on entire frameworks considered to be Lean.
The first proposed framework is game theory-based, where attackers and manufacturers are considered players within the game, with a reward function dictating the gain or loss for both parties. The Nash equilibrium is considered, and the likelihood of minimal damage with low cost and no critical threats is determined. The second framework is a resource allocation framework that optimally

minimizes the adverse effects of a future cybersecurity threat on Quality of Service (QoS) and production indices. The third framework is a predictive framework based on data analytics that is capable of detecting imminent attacks.
The practical aspects of these frameworks are discussed in this paper, along with a survey of technologies that optimize the efficiency of Industry 4.0, such as the Internet of Things (IoT), drones, robots, augmented reality, and machine learning. The authors highlight the waste generated due to cyber-attacks on these systems.
IoT is considered to have zero setup time and to reduce the production cycle, allowing for simpler processes, and data can be used to continually improve people and processes. Just-in-Time (JIT) manufacturing is integrated within IoT, helping to manufacture products using the right specifications with the right machines, materials, and people. The security problems that arise from attacks are the same as the security problems that come with the internet, such as authentication and access control, confidentiality, privacy, secure middleware, and trust.

Additive manufacturing technologies such as 3D Printing (3DP), Rapid Prototyping (RP), and Direct Digital Manufacturing (DDM) provide faster, more accurate prototyping, and remove the barriers of cost, distance, and time. Some of the security challenges in additive manufacturing are attacks on the STL files, attacks on the integrity of materials, and intellectual property theft.

Overall, this paper contributes to the understanding of the challenges and opportunities of implementing Lean and Six Sigma frameworks in the context of cybersecurity for Industrial 4.0 systems, providing insights and recommendations for future research and practice. [Shahin et al., 2020]

## IV. Case Study - Assignment 3

### A. Intel's implementation of NIST Cyber security framework

Intel is a leading company in the technology industry and has implemented the NIST CSF framework to enhance its cyber security. Intel has designed its framework into four categories: inbound materials, function development, enterprise and manufacturing, and outbound materials. To ensure that its products meet security objectives and technical standards, Intel has created the Security Development Lifecycle (SDL) which includes policies, procedures, tools, indicators, and consulting practices. This framework provides a comprehensive evaluation framework to protect personal information and prevent the inclusion of harmful software or hardware in their products. Intel has incorporated international standards such as ISO/IEC 27001, 27002, 27034-1, and 26036-3 to ensure that its SDL aligns with global standards. [Brown, ]

*1) Goals:* Intel recently created a Cybersecurity Framework to manage risk and increase insight into its risk picture. According to the organization, their experience with the Framework has helped to harmonize their risk management tools and terminology, resulting in more educated risk tolerance conversations within their organization. Furthermore, the Framework has improved Intel's capacity to establish security goals, create budgets, and deploy security solutions.

The pilot program produced a collection of reusable tools and best practices for analyzing infrastructure risk, which Intel intends to employ to extend its usage of the Framework. Intel launched a new business unit, the Intel Security Group, in early 2014, which merges all of its security resources into a single organization focused on increasing global security risk prevention.

Intel has exhibited leadership in enhancing cybersecurity throughout the global digital infrastructure by spending billions of dollars in software, hardware, services, and integrated solutions over the last decade. They also collaborate with partners from government, business, and non-governmental organizations to enhance cybersecurity in a way that encourages innovation.

*2) Design:* Intel separates its computational infrastructure into five essential business tasks for assessment: Design, Office, Manufacturing, Enterprise, and Services (DOMES). The Cybersecurity Framework has the ability to change cybersecurity on a global scale by concentrating on risk management rather than compliance. Overall, Intel's early experience with the Framework has been favorable, resulting in better risk management practices and security solutions.

Intel has developed its own grading system to measure the effectiveness of its NIST CSF framework. The grading system provides quantifiable data on risk, and two groups were used to score the matrix. Figure 3 displays the entire matrix and the deviation between the two groups, the core group, and subject matter experts (SME).

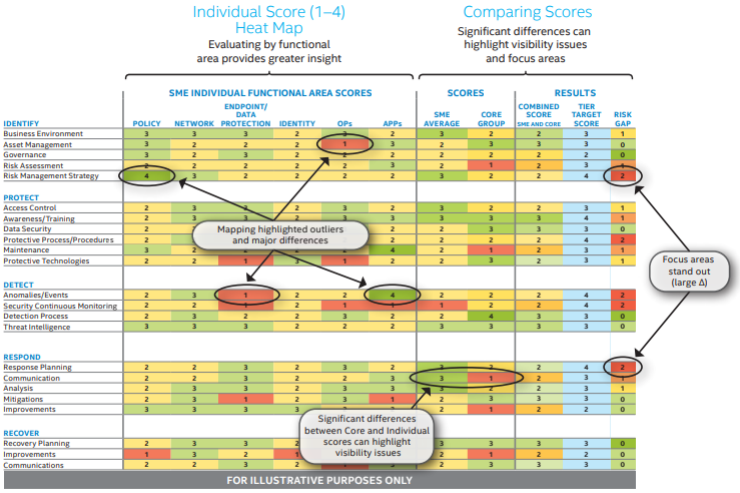



Figure 1. A heat map resulting from charting individual and group scores and their comparisons. *Note: The scores given are examples and not the actual scores.*

Fig. 3. Implementation Tiers for NIST CSF.

*3) Results:* Intel uses a table to determine the Tier selection score for each category, ensuring that they are maximizing their security measures while minimizing resource wastage. The development of their successful Framework pilot project cost under 175 full-time working employee hours [Casey, ], and Intel plans to expand this project to other areas of their essential business operations, such as Design, Manufacturing, and Services.

### B. Intel's implementation of Lean Six Sigma

*1) Overview and Business Case:* "The application of Lean Six Sigma (LSS) to configuration control in Intel's manufacturing R&D environment" describes Intel's LSS implementation and the resulting effects in the manufacturing Research and Development (R&D) department.
Lean Six Sigma (LSS) not only reduces waste, but also improves manufacturing processes, promotes innovation, and mass production. In Research and Development environments, process-focused strategies like LSS can improve "business processes" and allow innovators more time to think and create. The paper goes on to explain the LSS DMAIC (Define-Measure-Analyze-Improve-Control) framework implementation in Intel's Research and Development.
Intel applies Design-For-Manufacturing principles to manufacturing processes in order to attain design objectives and develop features

that can be manufactured in a high-volume setting. This requires integrating configuration control, statistical process control, and other methodologies into the R&D environment. Configuration control throughout Research and Development allows for the evaluation of risk, the collection of information, the tracking of changes to the intricate manufacturing processes required to produce the micro- and nano-features of processors, and the documentation of those changes.

The paper investigates how effectively LSS was integrated into Intel's configuration control procedure. Stopping inactive activities and standardizing production configuration control "business processes" were necessary to complete the project. The process included a process-walkthrough to assess the current state and collect baseline data, creating process maps to quantify waste and inefficiencies, defining the ideal state and a realistic target, selecting and implementing improvement actions, documenting the improvements, and creating and implementing a control plan to ensure the new process is sustained.

The project's efficiency advantages reduced the idle time by 60%, exceeding the target reduction of 40%. While maintaining the technical rigor of devising microscale and nanoscale manufacturing methods, stakeholder satisfaction increased. This case study illustrates how the LSS methodology can be utilized to improve R&D efficiency and company operations. [Panat et al., 2014]

The significance of configuration control in a research and development environment is further discussed in the paper, with a focus on the requirement for adequate documentation to support continuous learning and smart decision-making based on statistical data gathering and technical risk assessments. The success of R&D, particularly in manufacturing processes at the micro- and nanoscale, is stressed as being dependent on a strict configuration control procedure. It is said that the present configuration control procedure is extremely bureaucratic, with many checks and balances that lead to protracted wait times and poor White Papers. According to the author, putting Lean Six Sigma (LSS) principles into practice can improve stakeholder satisfaction, decrease defects, and remove non-value-added operations while saving money and time that more than offset the price of improving quality. In addition, there is a strong financial case for implementing LSS principles to improve the configuration control process.

*2) Define Methodology (DMAIC):* The authors of the study outline the process optimization efforts undertaken by an LSS team during the "Define" phase of the DMAIC methodology. To reduce unproductive waiting time and process variability, the team's objectives included plain and straightforward process flow, transparent transmission via appropriate connections, quick adjustments, and standardized operations. The team gathered information from customers, the business, and its employees in order to reduce or eradicate process steps that did not require substantial technological input.

To further elaborate, the authors of the study describe an LSS team that engaged in process improvement during the DMAIC's "Define" phase. The LSS technique stated that the team was comprised of a small number of competent R&D engineers who were stationed at the location where the process steps were taking place in order to collect the necessary data to enhance the process. The DMAIC process was given a deadline and a clear objective, namely to reduce process variability and idle wait time by 50% through structured and standard activities, clear transfer via ideal connections, straightforward and precise process flow, and small, quick changes. In order to determine the crucial process steps necessary for the WPs (Work Packages) for process improvements, the team first queried the process and gathered customer, business, and employee voices. To meet the goal of eliminating the idle time, the process stages that did not require essential technical input were identified for either significant reduction or complete deletion. The team was also given the task of comprehending both the business process's actual "what is" state and its ideal "what should be" state.

The team defined the "present" high-level process flow (shown in Figure 6) to indicate the configuration control process boundaries they wanted to improve. The configuration control software has two review forums and team member approvals. The activities are standardized but unstructured. Team members who write the modification and provide inputs also approve the WP in the computer system. In manufacturing R&D, stakeholders may include money, capacity, and technical fields including mechanical engineering, materials science, physics, chemical engineering, applied mechanics, and others. Changing the flow is difficult. Since there were so many stakeholders, the "one customer, one supplier, one method of information transfer" premise was not followed. The authors also found the WP's two review levels' formats inconvenient. Finally, the team members related the process complexity to technical rigor, meaning that they had not realized that "Technical difficult problems can be solved using simple business processes".

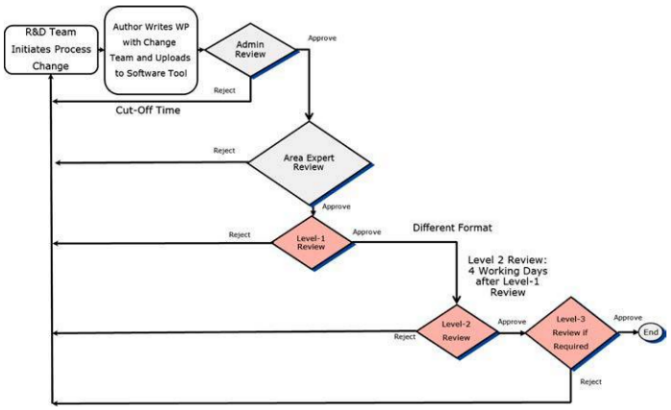



Fig. 4. High-level configuration control process flow for Intel's R&D environment

The team utilized a SIPOC table to identify client needs, process inputs, suppliers, and more. Furthermore, the team surveyed R&D engineers to evaluate configuration control process duration, satisfaction, and improvement ideas. This information helped estimate the WP process cycle and active time and informed future-state talks.

*3) Measure and Analyze:* In the measurement and analysis stage of DMAIC, the authors discuss the data gathered to measure baseline performance and analyze the root causes of any inefficiency or defect in the configuration control process. This is necessary for the success of Lean Six Sigma at Intel, as areas of waste and variation must have targeted solutions to address them. While exact numbers could not be disclosed, several figures were compiled based on the data to quantify and observe the configuration control process.

A SIPOC diagram was first created to identify all the relevant elements of a process improvement project before it begins, and by using it to collect baseline data from the R&D engineers about the time required in the configuration control process, a process map was created to graphically depict the inputs, actions, and outputs of each process. In this case, the authors also edited each process as value-adding (VA) or non-value-adding (NVA), where all NVA processes are time spent waiting by the engineers for feedback or confirmation. On average, a VA process would take 0.5 units of time, while an NVA process would take at most 40 units of time. The exact unit is undisclosed due to confidentiality by Intel, but this depicts an extremely large amount of time wasted in a process that is not productive.

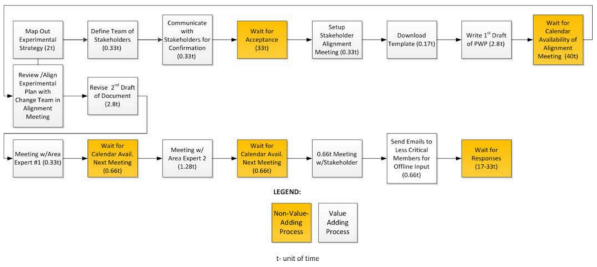



Fig. 5. Process Map

Next, the authors constructed a Pareto chart to display customer priorities in order of their frequency. This naturally distributes more frequent priorities towards the top of the chart, annotating significance and areas for improvement and process streamlining. The leading customer priority is the time spent by the first and final approving forum. The least value was placed on forecasting, email waiting, and offline meetings.

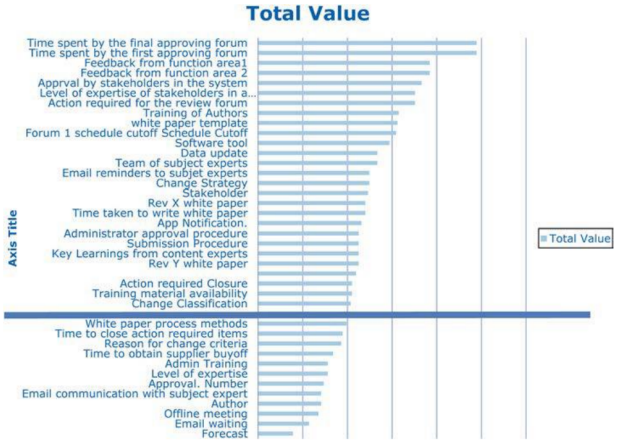



Fig. 6. Pareto Chart

Based on the information in the Pareto chart, the authors did a failure-modes-and-effects-analysis (FMEA) to predetermine possible areas for failure and possible corrective measures that can be taken to overcome these issues before they arise. Calculating Risk Priority Numbers (RPN) helped them prioritize fixing high-risk processes and identify process deficiencies in line with Lean Six Sigma standards, without which these issues could not have been identified. For example, the excessive wait times identified from the Pareto chart were prioritized and eliminated by making a simpler process flow. This helped the research and development team at Intel bypass NVA processes that reduced the efficiency of a technical team with non-technical details that are not relevant to their jobs but are part of the larger system.

*4) Improve:* In section 3.3 FMEA was used to prioritize the improvement actions based on the higher RPN scores, to establish a "wait time" versus "time required for the change based on the process map created by walking the process". This was done to simplify the process, reduce idle time and control the diversity in output in a better manner. For this, there were certain actions including

1) "Not depending on approval from the team of area experts" which reduced a redundant activity and thus, waiting time.
2) "WP Quality and content feedback before review" reduced the communication time and helped in technical evaluations as well. Variation in "human temper" of the members was also reduced.
3) "Reducing the time difference between different levels of review forums" ensured a balance between the wait times of the change/WP owners and the time required by the reviewers. It helped authors in reducing the NVA time.
4) Consolidation of technical are experts/groups, by deciding on a single point of contact for a given technical area for feedback to the change owner. This also reduced NVA time drastically.
5) Creating WP tracking sheets reduced WP quality variation. It ranked the changes in terms of a set rubric. This helped recognizing change owners with a good score and mentoring those with poorer ones.
6) Creating universal standard WP templates reduced variability and confusion in the business process, helping reduce the number of reworks and hence saving time from the WP cycle.

*5) Controls:* The configuration control process changes were taught to RD teams through training material and courses. Additional training was given to first-time authors. Software tools were created to track corrective actions, and owners were assigned to ensure implementation. Quality was monitored continuously through a tracking sheet, which can be used to introduce measurable improvements. These changes resulted in improved technical content quality and reduced WP review time.

### C. Discussion

Combining the Lean Six Sigma (LSS) and National Institute of Standards and Technology (NIST) methodologies might result in considerable benefits for businesses. While each framework has its own set of advantages and disadvantages, merging them might result in a more complete and effective framework for optimizing procedures and assuring security.

There is presently no link or integration between LSS and NIST, as evidenced by the two case studies mentioned in above. Integrating the two frameworks might provide organizations with a more unified and efficient approach to enhancing operations and safeguarding their systems. The better synergy between process improvement activities and cybersecurity measures would result in more effective risk management overall.

Data analysis and measurement are important aspects of both LSS and NIST. Organizations might use data and analytics to find possibilities for improvement and assess the efficacy of their security measures by combining these techniques. More data-driven decision-making would ensue, which is crucial in today's digital world.

Another advantage of integrating LSS and NIST is that eliminating waste and errors may improve security and risk management. The two frameworks can complement one another and collaborate to attain these objectives.

Finally, both the LSS and NIST frameworks are extensively used in a variety of businesses and areas. Organizations might give a single vocabulary and shared knowledge of process improvement, risk management, and quality control by merging these frameworks. This would enable increased collaboration and cooperation among departments and stakeholders, resulting in improved overall outcomes.

## V. Analysis

### A. Identifying Lean within NIST CSF

The aim of this paper is to identify key elements of lean within the NIST framework functions and use the function of CSF to improve waste management. The NIST framework is designed for different types of organizations, and it divides them into four tiers

based on their risk profile. The adaptive tier is the most secure as it encompasses all three elements shown in figure 8.

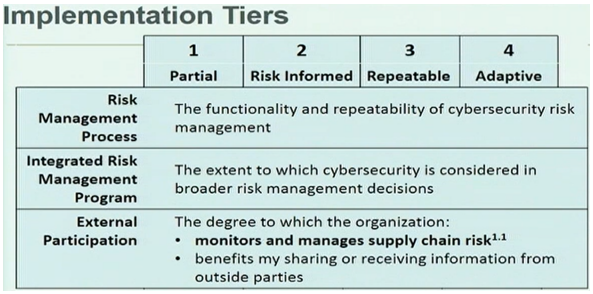



Fig. 7. Implementation Tiers for NIST CSF.

When considering lean for your organization, it is crucial to take into account the tier your organization falls into. Implementing an ambitious security plan that is not necessary for your risk level would be a waste of resources and could disrupt other value chains within the organization.

The CSF functions of identify, protect, detect, respond, and recover are important for waste management, and the implementing party assigns a risk value to each subcategory within these functions. We can also isolate the three types of waste we have discussed in our literature review: Muda, Mura, and Muri. The decision of implementing a category would not only depend on the risk level but also its importance in waste management.

The value components within the framework include data (such as personally identifiable information, intellectual property, and confidential documents) and physical (including employee and product safety). The value stream includes the supply chain and value subprocesses.

A cyber attack can generate waste that could have been avoided if necessary precautions had been taken. Hence, it is essential to have procedures in place to reduce waste. We have categorized the different functions of waste and explained them using examples. The table below shows the three types of waste and the counter phrases that help reduce them. These counter phrases have been specifically selected from the literature review and the NIST document to classify all subcategories of the CSF.

| Waste Category | Keywords | Counter-Phrases |
|---|---|---|
| **Muda** (Non-Value-Adding) | Waste, Inefficiency, Unnecessary | Planning, Categorize, Design, Standardize, Simplify |
| **Mura** (Inconsistency) | Variability, Unpredictability | Standardize ,Streamline, Balance, Stabilize, Align |
| **Muri** (Overburden) | Overload, Strain, Stress | Contribute, Optimize, Automate, Balance, Prioritize, Reschedule |

Fig. 8. Counter phrases use to classify the subcategories of NIST CSF.

For Muda waste, which refers to non-value-adding tasks, terms like planning, categorizing, and design can help reduce waste. For example, the Cyber supply chain risk management processes that are established can help manage risk and mitigate threats. By having a way to manage risk (ISO 28001), less waste is generated in an event like a cyber attack as the threat is already mitigated due to the procedures in place.

For Mura waste, which refers to inconsistency, we have terms like streamline, balance, and stabilize to describe its improvement. One of the subcategories describing threat intelligence is shared on forums, this allows a collaborative environment for development. One of the most famous tools is virus total which saves millions of malware signatures, hence if anyone gets infected with a known malware there are already fixes for this malware. External and internal collaboration save time by everyone is working on a task that they are good at.

Muri waste can be reduced in cybersecurity processes by optimizing workflows and automating tasks. This can be achieved through the use of tools such as security orchestration, automation, and response (SOAR) platforms that automate repetitive tasks and enable faster incident response. Establishing clear roles and responsibilities for cybersecurity across the entire workforce and third-party stakeholders can also help distribute the workload and ensure everyone is working on tasks that align with their skills.

Automation tools such as anti-viruses, intrusion detection and prevention systems, and firewalls can also help reduce Muri waste by automating routine security tasks and freeing up time for more complex tasks that require human expertise. By leveraging these tools, cybersecurity teams can more effectively manage their workload and focus on high-value activities that require specialized knowledge and skills.

Block diagrams for all of the functions are available in the appendix for more clarity.

## VI. Conclusion

We started by defining the two frameworks, then we did a comprehensive literature review to isolate the use cases of the two frameworks. Then we identified Lean design within the NIST CSF. after which we described and implementation of the new framework. Cyber attacks cause a lot of damage to an organization, hence designing a good framework is necessary. But the emphasis has to be made on adopting a CSF that does not disrupt other value chains. Security should be at the heart of everything but should be so seamless that no one would recognize it.

## VII. Future Work

For our future work, we can focus on identifying Lean design in different standardized cyber security implementations such as ISO 27001. our main aim would be to assign a waste value to the different procedures to see how much which elements have the greatest cost for the value they provide. Also, we can compare and contrast the generation and reduction of waste within cyber security. Cyber security might be generating waste by hindering a sub-value chain while also protecting sub value of the product.

## REFERENCES


[Ahmad et al., 2018] Ahmad, M. O., Dennehy, D., Conboy, K., and Oivo, M. (2018). Kanban in software engineering: A systematic mapping study. *Journal of Systems and Software*, 137:96–113. doi:10.1016/j.jss.2017.11.045.

[Belkadi et al., 2019] Belkadi, S., Cherti, I., and Bahaj, M. (2019). Lean in information technology: Produce the human before the software. *Advances in Intelligent Systems and Computing*, page 203–213. doi: 10.1007/978-3-030-11881-$5_17$.

[Brown, ] Brown, D. A. Best practices in cyber supply chain risk management - nist. url: https://www.nist.gov/system/files/documents/itl/csd/NIST$_U SRP - Intel - Case - Study.pdf$.

[Casey, ] Casey, T. A cybersecurity framework use case intel corporation. url: https://supplier.intel.com/static/governance/documents/The-cybersecurity-framework-in-action-an-intel-use-case-brief.pdf.

[Dubbaka and Dadkhah, ] Dubbaka, B. and Dadkhah, S. P. Role of information technology in lean enterprise systems - diva portal. url: https://www.diva-portal.org/smash/get/diva2:1312034/FULLTEXT01.pdf.

[Fox, 2023] Fox, J. (2023). Top cybersecurity statistics to know for 2023. url: https://www.cobalt.io/blog/cybersecurity-statistics-2023.

[Hsieh et al., 2007] Hsieh, C.-T., Lin, B., and Manduca, B. (2007). Information technology and six sigma implementation. *Journal of Computer Information Systems*, 47(4):1–10. doi: 10.1080/08874417.2007.11645975.

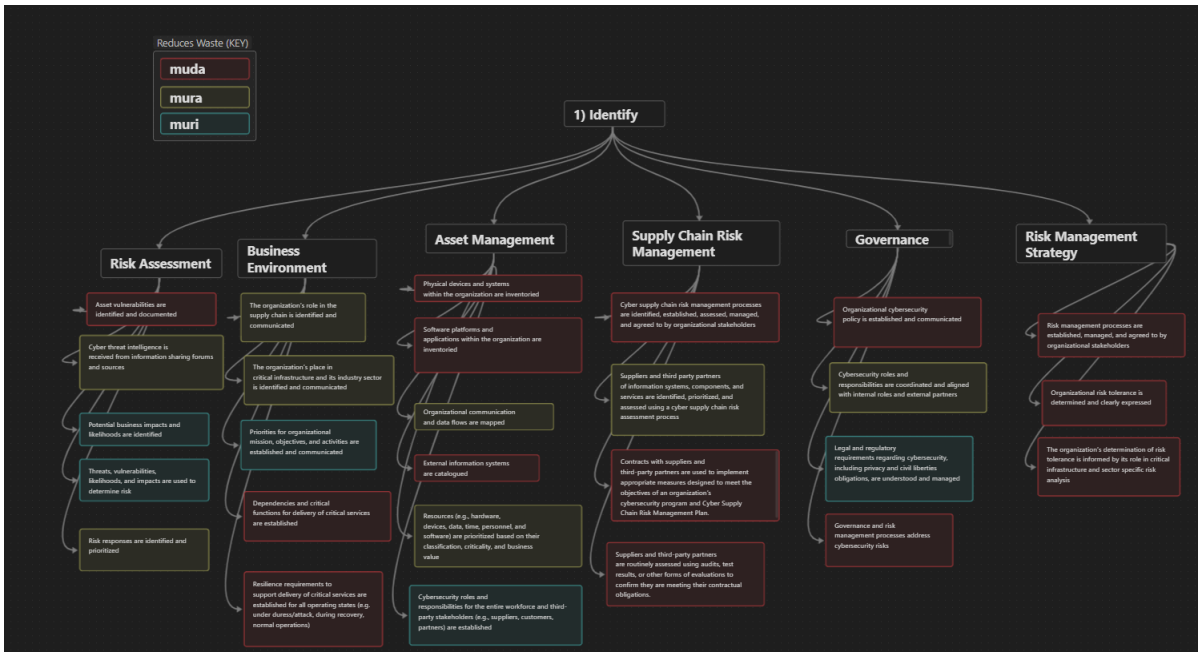
[Kessel, ] Kessel, P. v. Poka-yoke – japanese for cybersecurity professionals. url: https://www.linkedin.com/pulse/poka-yoke-japanese-cybersecurity-professionals-paul-van-kessel/.

[Panat et al., 2014] Panat, R., Dimitrova, V. I., Selvamuniandy, T., Ishiko, K., and Sun, D. (2014). The application of Lean Six Sigma to the configuration control in Intel's manufacturing Ramp;D environment. *International Journal of Lean Six Sigma*, 5(4):444–459.

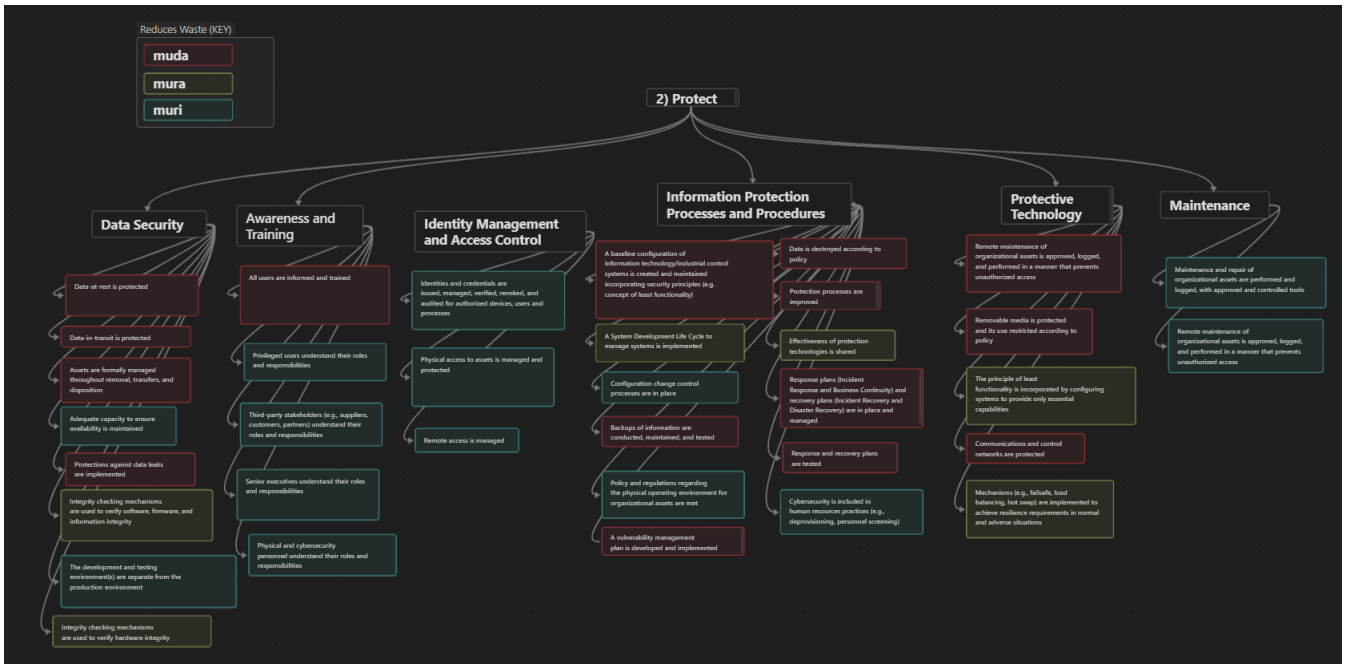
[Riezebos et al., 2009] Riezebos, J., Klingenberg, W., and Hicks, C. (2009). Lean production and information technology: Connection or contradiction? *Computers in Industry*, 60(4):237–247. doi: 10.1016/j.compind.2009.01.004.

[Shahin et al., 2020] Shahin, M., Chen, F. F., Bouzary, H., and Zarreh, A. (2020). Frameworks proposed to address the threat of cyber-physical attacks to lean 4.0 systems. *Procedia Manufacturing*, 51:1184–1191. doi: 10.1016/j.promfg.2020.10.166.

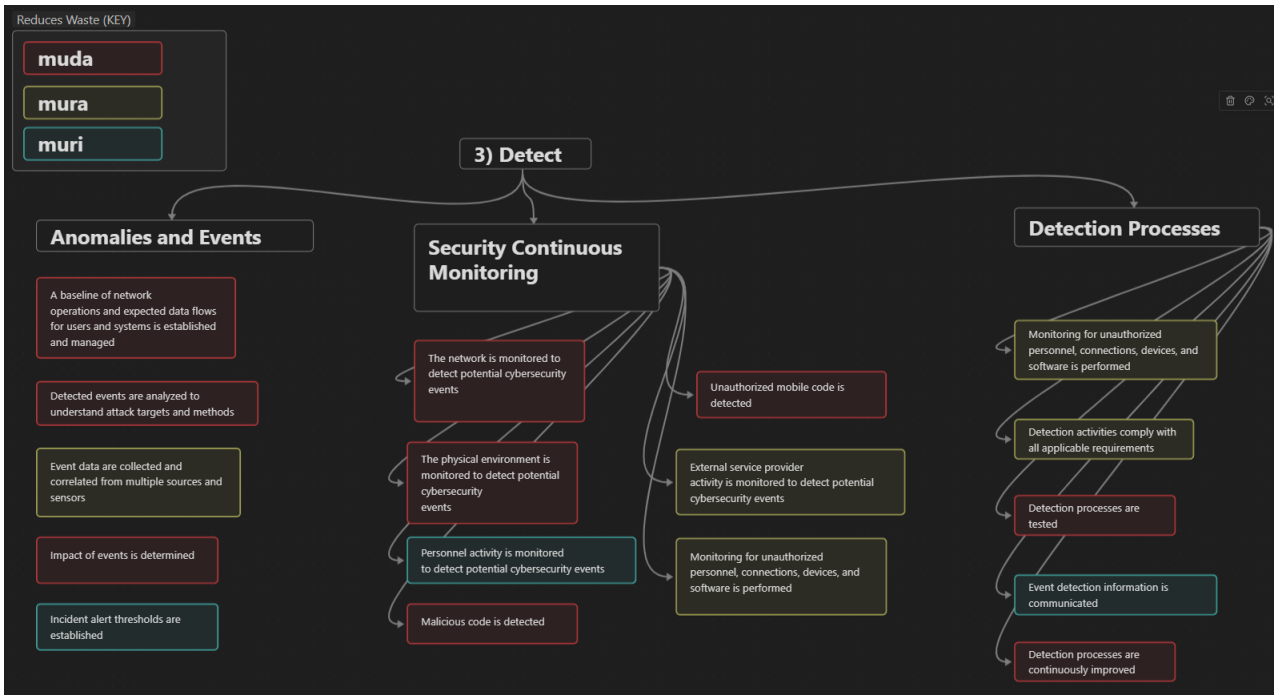
# VIII. Appendix



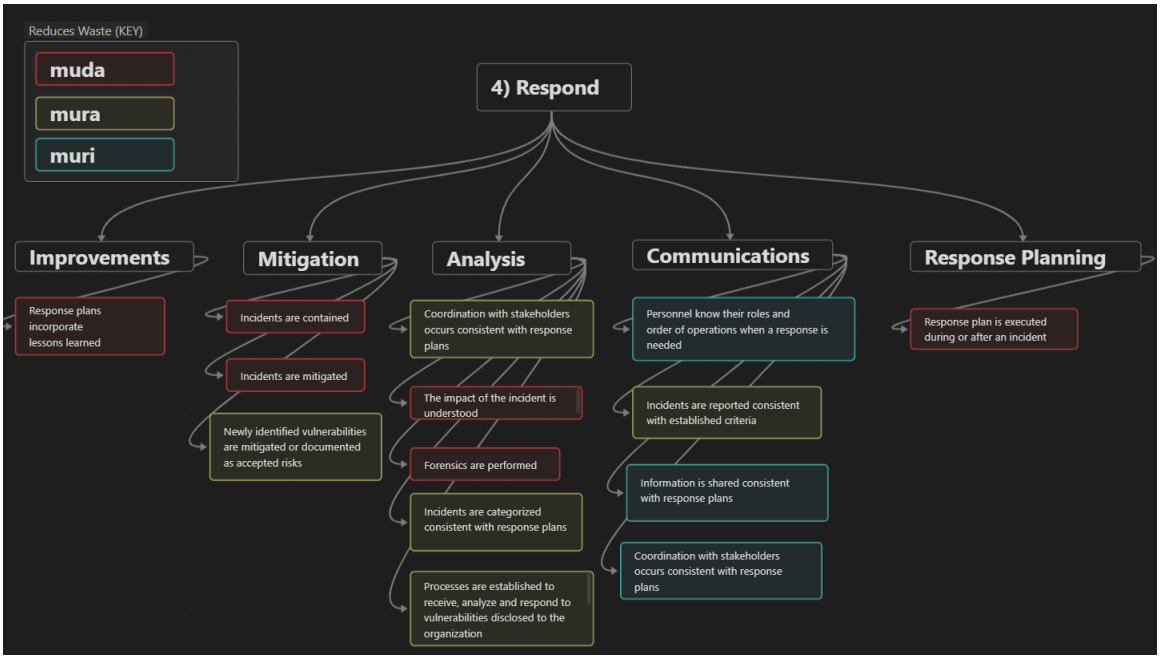

One of the functions of CSF is to identify which defines the necessary assets that have to be protected. We are categorizing all identified subcategories with the different waste that it improves.



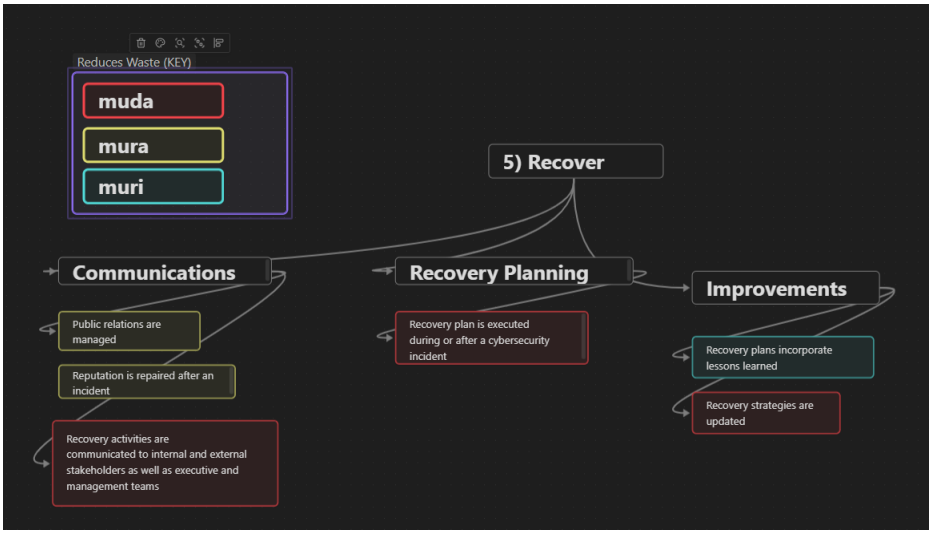

One of the functions of CSF is to protect which is the necessary process that help in protecting the assets. We are categorizing all identified subcategories with the different waste that it improves.




One of the functions of CSF is to detect which defines the necessary procedures to monitor and find anomalies. We are categorizing all identified subcategories with the different waste that it improves.




One of the functions of CSF is to respond which defines the necessary procedure to mitigate and analyze attacks. We are categorizing all identified subcategories with the different waste that it improves.




One of the functions of CSF is to recover which defines the necessary planning and improvements to recover from and attack. We are categorizing all identified subcategories with the different waste that it improves.

**Table 1. Customized Tier Definitions**

| FOCUS AREA | TIER 1 PARTIAL | TIER 2 RISK INFORMED | TIER 3 REPEATABLE | TIER 4 ADAPTIVE |
|---|---|---|---|---|
| People | • Cybersecurity professionals (staff) and the general employee population have had little to no cybersecurity-related training.<br>• The staff has a limited or nonexistent training pipeline.<br>• Security awareness is limited.<br>• Employees have little or no awareness of company security resources and escalation paths. | • The staff and employees have received cybersecurity-related training.<br>• The staff has a training pipeline.<br>• There is an awareness of cybersecurity risk at the organizational level.<br>• Employees have a general awareness of security and company security resources and escalation paths. | • The staff possesses the knowledge and skills to perform their appointed roles and responsibilities.<br>• Employees should receive regular cybersecurity-related training and briefings.<br>• The staff has a robust training pipeline, including internal and external security conferences or training opportunities.<br>• Organization and business units have a security champion or dedicated security staff. | • The staff's knowledge and skills are regularly reviewed for currency and applicability and new skills, and knowledge needs are identified and addressed.<br>• Employees receive regular cybersecurity-related training and briefings on relevant and emerging security topics.<br>• The staff has a robust training pipeline and routinely attend internal and external security conferences or training opportunities. |
| Process | • A risk management process has not been formalized; risks are managed in a reactive, ad hoc manner.<br>• Business decisions and prioritization are not factored into risk and threat assessments.<br>• Risk and threat information is not communicated to internal stakeholders. | • Prioritization of cybersecurity activities is informed by organizational risk objectives, the threat environment, or mission requirements.<br>• Risk-informed, management-approved processes and procedures are defined and implemented, and the staff has adequate resources to perform its cybersecurity duties.<br>• Cybersecurity information is shared within the organization on an informal basis.<br>• Management has approved the risk management practices, but these practices may not have been established as organizational-wide policy. | • Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business or mission requirements and a changing threat and technology landscape.<br>• Consistent risk management practices are formally approved and expressed as policy, and there is an organization-wide approach to manage cybersecurity risk.<br>• Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. | • Cybersecurity risk management is an integral part of the organizational culture.<br>• The organization actively adapts to a changing cybersecurity landscape, evolving and sophisticated threats, predictive indicators, and lessons learned from previous events in a timely manner.<br>• The organization continually incorporates advanced cybersecurity technologies and practices.<br>• There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures. |
| Technology | • Tools to help manage cybersecurity risk are not deployed, not supported, or insufficient to address risks.<br>• Tools may be in place but are not adequately tuned or maintained.<br>• Technology deployed lags current threats.<br>• Tool deployment may not adequately cover risk areas. | • Tools are deployed and supported to address identified risks.<br>• The tools in deployment are tuned and maintained when resources are available.<br>• The technology deployed, for the most part, keeps pace with current threats.<br>• Tool coverage of the risk area is complete when deployed. | • Metrics are used to evaluate the usefulness and effectiveness of the deployed tools.<br>• The tools in deployment are routinely tuned and maintained.<br>• The technology deployed keeps pace with current and emerging threats.<br>• Tool coverage of the risk area is complete and updated as changes are recognized. | • The tools deployed in the environment are regularly reviewed for effectiveness and coverage against changes in the threat environment and internal ecosystem.<br>• The tools and technology deployed anticipate emerging threats. |
| Ecosystem | • The organization does not understand its role in the larger ecosystem or act accordingly.<br>• The organization does not have processes in place to participate in or collaborate with external organizations on cybersecurity issues. | • The organization knows its role in the larger ecosystem but has not formalized its capabilities to interact and share information externally.<br>• The organization may participate in or collaborate with external organizations on cybersecurity issues on an ad hoc basis. | • The organization understands its ecosystem dependencies and partners and can act accordingly when it receives information from these partners. | • The organization manages risk and actively shares information with partners to ensure that accurate, current information improves ecosystem cybersecurity before events occur. |

Intel Tiers that define the scoring method