المركز الوطني للأمن السيبراني
National Cyber Security Center

Cybersecurity Framework Booklet

¢ ĸ Ŝ a ŀ ƛ ƴ / ŀ LJ ŀ ō ƛ
b ŀ ű ƛ ƨ ƴ ŀ f / è ō ŜNJ ă

A Comprehensive View

The National Cybersecurity Framework of the Hashemite Kingdom of Jordan

Contents

Jordan National Cybersecurity Framework Capabilities 3

1 Security in Architecture and Portfolio 5

1.1 Strategy Management 6

1.2 Enterprise Architecture Management 9

1.3 Portfolio Management 12

[illegible] Service Product Portfolio 15

2 Security in Development 17

[illegible] Requirements Management Capability 19

[illegible] Product & Team Backlog Capability 22

2.3 Service/Product Design Capability 24

2.4 Secure Code Management Capability 27

2.5 Test Management Capability 29

2.6 CI/CD Pipeline Capability 33

[illegible] Defect Management Capability 36

2.8 Build Management Capability 40

2.9 Release Management Capability 43

3 Security in Delivery 46

3.1 Resource Management 47

3.2 Automated Remediation 50

3.3 Request Management 53

3.4 Change Management 56

3.5 Identity & Access Management 59

3.6 Deployment/Provisioning 62

3.7 Secrets Management 65

3.8 Operations Management 68

4 Security in Operations 71

4.1 Incident Management Capability 73

4.2 Problem Management Capability 77

4.3 Event Management Capability 80

4.4 Security Monitoring Capability 84

4.5 Configuration Management Capability 88

4.6 Fraud & Forensics Investigations Capability 91

4.7 Continuity Management Capability 93

4.8 Threat Intelligence Capability 98

4.9 Data Management Capability 100

4.10 Service Level Management Capability 105

5 Fundamental Capabilities 108

5.1 Policy Management Capability 110

5.2 Risk & Compliance Capability 113

5.3 IT Audit Management Capability 116

5.4 Vendor & Contract Management Capability 118

5.5 Workforce Management Capability 120

[illegible] Legal Management Capability 122

5.7 Facility Management Capability 124

5.8 Intelligence & Reporting Capability 126

6 Security in National Cyber Responsibility 128

Jordan National Cybersecurity Framework Capabilities

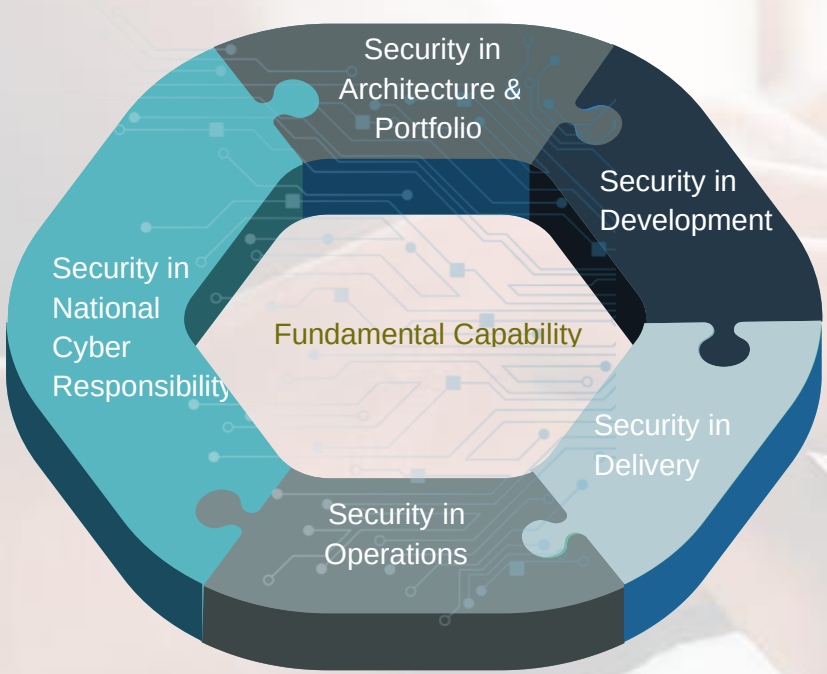
The Jordan National Cybersecurity Framework requires all entities, private and government, to build and develop essential capabilities that will ensure the optimal utilization of the national as well as promoting digital transformation strategy and resources to elevate the cybersecurity maturity index. These capabilities, along with their related capabilities and sub capabilities have all put into integrating with the aim of ensuring cybersecurity.

To provide an enlightenment view of these main capabilities, the following is brief for each:

- **Security in Architecture & Portfolio:** Security in Architecture is the first capability in Jordan's National Cyber framework, and it is considered one of the most important capabilities, given its precedence in application and importance in integration with the rest of the capabilities to maintain security and maximum protection for entities, as it is one of the most critical planning features of any project or producer's planning stage, enabling effective prioritization of proposed investments, initiatives, and projects.
- **Security in Development:** The measures and techniques used during the development process to ensure that the resulting system is secure and protected against potential threats, and this includes practices such as vulnerability assessments, security testing, and adherence to industry-standard security protocols and guidelines.
- **Security in Delivery:** Security in Delivery refers to the measures taken to protect data and services during transformation and delivery. Such measures include secure encryption, tracking and monitoring systems, and personnel background checks. Delivery security aims to ensure that service/data are delivered to the intended recipient safely and securely without being lost, stolen, or tampered with during transit.
- **Security in Operations:** Security in operations refers to the practices and processes that aim to protect an entity's services and information systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. These operations encompass a wide range of activities, such as incident response, threat intelligence, vulnerability management, and so on.
- **Foundational Capabilities:** Fundamental capabilities in cybersecurity are the foundational skills and knowledge that entities and individuals must have in order to effectively protect their services, systems, networks, and data from unauthorized access, misuse, and malicious attacks. These capabilities are essential for ensuring the service resiliency and confidentiality, integrity, and availability of information, which are the three main pillars of information security.

- **Security in National Cyber Responsibility:** Cybersecurity is a collective responsibility shared between countries, businesses, academia, and individuals. Countries worldwide are increasingly realizing the importance of cybersecurity in protecting national security and its significant impact on economic growth.

The capabilities are combined to create a foundation that equips institutions with fundamental concepts to enhance their knowledge in the field of cybersecurity. In the Jordan National Cybersecurity framework, the following sequence is used to describe these capabilities:



The ensuing exposition presents a comprehensive overview of the capabilities, taking into account the salient features of each while enlisting the related sub-capabilities of each of the principal capabilities. It is intended to offer a concise and lucid summary of the capabilities and sub-capabilities in a comprehensible and coherent manner to readers.

1 Security in Architecture and Portfolio

Security in Architecture is the first capability in Jordan's National Cyber framework, and it is considered one of the most important capabilities, given its precedence in application and importance in integration with the rest of the capabilities to maintain security and maximum protection for entities, as it is one of the most critical planning features of any project or producer's planning stage, enabling effective prioritization of proposed investments, initiatives, and projects.

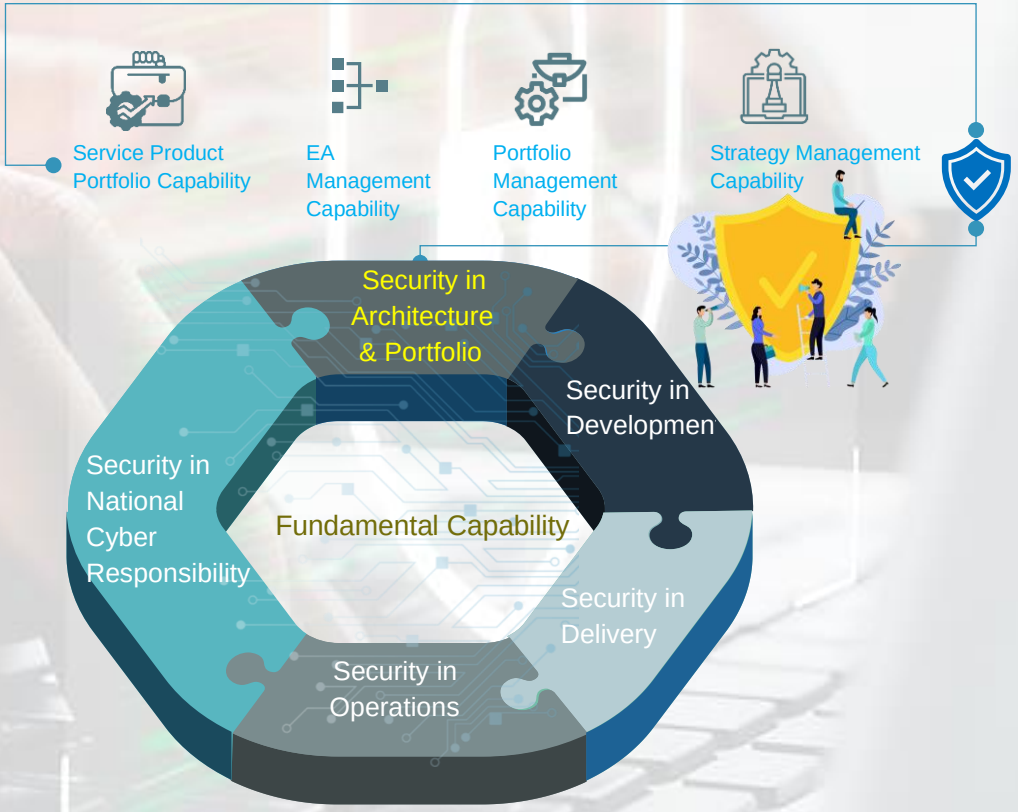
It is intended to improve security by designing strategically and comprehensively. It is the Strategy to Portfolio function that allows for the efficient design, creation, traceability, and management of secure, strategy aligned products/services or enhancements. From a strategic standpoint, develop a security and cybersecurity strategy aligned with the overall business strategy. Assuring the practice of articulating and modeling cybersecurity within enterprise architectures. As a result, optimize the required security among products/services by managing portfolio security and cyber security aspects.

To have this consolidating capability, each entity must use the main underlying capabilities at the appropriate maturity level, which are concisely listed below:

- **Strategy Management Capability:** This capability involves ensuring the strategic control and management of Cybersecurity and Cyber Risk across all Services and Information, from top management to everyone.
- **Enterprise Architecture Management Capability:** This capability focuses on articulating and modeling the entire business from all angles to ensure proper, optimized, by-design, and effective security architectures.
- **Portfolio Management Capability:** Portfolio management seeks to maximize returns while minimizing risk. As a result, cyber risk would be considered at an early stage to ensure action rather than reaction with cost optimization.
- **Service Product Portfolio Capability:** This is a supplementary capability to the overall portfolio management capability, and it manages the level of detail for each product or service. To ensure that security by design is implemented in each service or product, as well as proper risk, technology, and resource classification, to achieve the required CIAS index.

A Comprehensive Overview

The following exposition provides a comprehensive overview of this main capability and its sub-capabilities among its counterparts, followed by a brief explanation. This overview is intended to serve as a valuable reference for understanding this critical capability and its underlying sub-capabilities.



1.1 StrategyManagement

A cybersecurity strategy management capability is the ability of an entity to develop, implement, and maintain a comprehensive cybersecurity strategy that aligns with the entity's overall business objectives and protects the entity's information assets and services. A robust strategy management capability requires a clear understanding of the entity's risk tolerance, threat landscape, and business priorities. It involves the development of a detailed cybersecurity strategy that outlines the entity's approach to managing cybersecurity risks, including identifying and protecting critical assets, detecting and responding to cyber threats, and recovering essential functions of business in the event of a cyber incident.

The strategy development process should involve key stakeholders, including senior management, IT, legal, and risk management, to ensure the strategy aligns with the entity's overall business objectives and risk management framework. Once the cybersecurity strategy is developed, it must be implemented through various initiatives, including security awareness training, vulnerability management, incident response planning, and deploying security technologies. A robust governance framework is necessary to ensure that the strategy is implemented effectively and the progress is tracked against goals and objectives. Effective metrics and reporting are critical to measuring the effectiveness of the cybersecurity strategy. This includes tracking progress against goals and objectives, reporting to senior management and other stakeholders, and conducting regular reviews to ensure the strategy remains effective and current.

Security Strategy & Goals

Security strategy and goals in cybersecurity refer to an entity's ability to define and implement a comprehensive cybersecurity strategy that aligns with the entity's overall objectives and goals. This includes setting clear cybersecurity goals, establishing a risk management framework, and implementing appropriate controls to mitigate cybersecurity risks.

Here are some key potentials required for effective security strategy and goals in cybersecurity:

- **Define Clear Security Goals:** An entity needs to define clear and measurable security goals that align with the overall business objectives. This helps ensure that cybersecurity efforts are focused on protecting the most critical assets and operations.
- **Develop a Comprehensive Security Strategy:** A comprehensive security strategy should be developed that addresses all aspects of cybersecurity risk management, including people, processes, and technology. This includes defining the entity's risk management framework and developing cybersecurity policies, procedures, and guidelines.
- **Integrate Security Within Business Objectives:** An effective security strategy should be integrated within the entity's objectives so that security measures are designed to support and enable business

operations. This requires strong collaboration and communication between the cybersecurity team and the business units.

- **Implement Appropriate Security Controls or Activity**: The security strategy should include a set of proper security controls or activities to mitigate the identified risks. These controls or activities may include technical controls such as firewalls, intrusion detection and prevention systems, encryption, and administrative and physical controls, But it has to include the non-technical controls such as awareness, capacity building, governance, process solidifications and/or reengineering.
- **Monitor and Assess Security Performance**: Effective security strategy and goals capabilities require ongoing monitoring and assessment of security performance to ensure the controls are adequate and aligned with the business objectives. This may include business and functional tabletop exercises, testing threat modeling scenarios, regular audits, vulnerability assessments, and penetration testing.
- **Continuously Improve Security**: Cybersecurity threats constantly evolve, so it is essential to continuously improve security capabilities in response to changing threats and risks. This requires a culture of continuous improvement and a process for identifying and addressing emerging threats and vulnerabilities.

In conclusion, a strong security strategy and goal setting capabilities are crucial for controlling cybersecurity risks and protecting an entity's critical assets and operations. This necessitates a comprehensive approach including all stakeholders, as well as a significant emphasis on integrating cybersecurity activities with business objectives.

Zero Trust Strategy

Zero trust is one of the fundamental concepts that is widely adopted in the cybersecurity world. The Zero Trust Architecture approach is commonly used at the Technology and application layers, where all network and traffic transactions are treated as threats to be examined and never just simply trusted and must be checked every time and everywhere. This concept should also be adopted in the strategy and business architectures for checking, verifying, and validating that the entity will have the required business, functional, and role components to achieve its Strategic Goals, Objectives and Services.

Strategy Management prerequisites (Process, People)

Several key prerequisites for effective Strategy Management include process and people.

- **People**: People are a critical prerequisite for a successful strategy management capability in cybersecurity. This includes having the right personnel with the necessary skills, knowledge, and expertise to develop and implement a comprehensive cybersecurity strategy. Additionally, it is important to have a strong leadership team that can provide direction and oversight and engage all stakeholders across the entity.
- **Process**: Process is another critical prerequisite for a successful strategy management capability in cybersecurity. This includes having a comprehensive Enterprise Architecture framework in place, as well as a defined process for identifying business objectives, key performance, and risk indicators, as well as assessing, measuring, and prioritizing cybersecurity risks. Additionally, it's important to have a clear and well-defined governance structure to ensure that all stakeholders are engaged and informed throughout the process.

In summary, a successful strategy management capability in cybersecurity requires the right people and well-defined processes to implement and monitor the strategy. By ensuring these prerequisites are in place, entities can better protect themselves against cybersecurity risks and threats.

The Benefits of Applying Strategy Management Capability

Incorporating this capability within entities will yield a multitude of benefits, such as:

- **Clear Direction**: A well-defined cybersecurity strategy gives the entity clear direction and priorities for its cybersecurity efforts. This ensures that resources are allocated effectively and cybersecurity risks are managed appropriately.
- **Better Alignment with Business Objectives**: A cybersecurity strategy that is aligned with the entity's overall business objectives ensures that cybersecurity is integrated into the entity's operations and that cybersecurity risks are managed in a way that supports the entity's goals.
- **Improved Risk Management**: A cybersecurity strategy enables the entity to identify and prioritize cybersecurity risks and to allocate resources accordingly. This ensures that cybersecurity risks are managed effectively and the entity's information assets are protected.
- **Better communication**: A cybersecurity strategy enables better communication between cybersecurity teams and other business functions. This ensures that cybersecurity risks are understood and managed effectively across the entity.

1.2 Enterprise Architecture Management

Enterprise Architecture is one of the most important capabilities that works as a foundation for the other capabilities mentioned in this framework to ensure reliable security by design. It plays a fundamental and critical Prerequisite for the cybersecurity program to be established, operated and maintained.

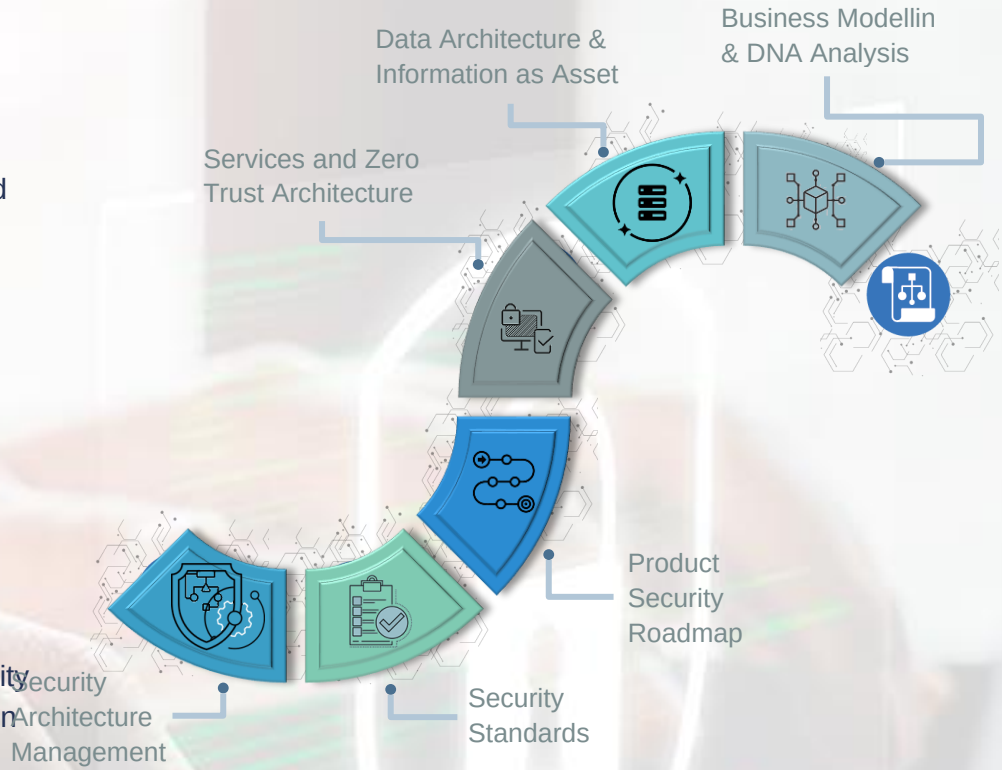
entities Asking and answering the six golden questions (Why, How, who, what, where, and when) related to their business, functional elements and components will be able to identify and develop the fundamental robust and integrated business artifacts

- Strategy and Goals
- Roles and Responsibilities
- Locations and Geography
- Policies, Processes, Procedures and Activi
- Things and materials
- Events and Triggers.

Understanding, Modelling, and analyzing the abovementioned Business artifacts will enable the Business leaders, Risk managers, Cybersecurity Managers as well as the Digital Transformation leaders to build a common understanding of the business nature and to integrate both the Digital Transformation and Cybersecurity strategies and to map the entity KPIs and KRIs, and to select the most efficient and effective cybersecurity Controls.

Government and Private Entities are required to develop, update, and maintain the major architecture, which reflects:

- Business Architecture
- Strategy Architecture
- Services and Cross-Functional Architecture
- Data & Information Architecture
- Application and Technology Architecture
- Security Architecture



Business Modelling & DNA Analysis

All operational business processes and cycles should be captured, modeled, and linked with the entity al structures, exposed services, products, data and information, customers, interfaces, internal flows of information and potential risk points. The Business modeling must show all different possible paths and scenarios, different business events, and different business data objects. Although business models might be developed using different and various tools, the Open Group free-to-use ArchiMate modeling language is highly recommended to develop a national and common understanding of the National Digital Business Services and National Data Catalogue, which will provide foundational practices for the National Resiliency.

The detailed Entity DNA Analysis will come once all the above are modeled and maintained. The 360 views of each element and both the content and context analysis of the business artifacts will provide a massive business matrix analysis for comprehensive and detailed cyber risk management, analysis, measurement.

Data Architecture & Information as Asset

Data and Information are the most important assets to be protected from any breach or misuse that might cause economic, financial, or any adverse National Impact. Therefore, the Data and Information Architecture should be Developed, modeled, analyzed, and Maintained, and it should cover the data objects along each of the core layers and with the different system part interactions This capability is linked and attached to the Data Management Capability. The data models and data architecture should be defined comprehensively from different points of view to show a full link between the data objects in any layer or dimension covering the full data lineage

Services and Zero Trust Architecture

Zero trust is one of the fundamental concepts that is widely adopted in the cybersecurity world. The Zero Trust Architecture approach is commonly used at the Technology and application layers, where network and traffic transactions are treated as a threat to be examined and never just simply trusted and must be checked every time and everywhere. This concept should also be adopted in the strategy and business architectures for checking, verifying, and validating that the entity will have the required business, functional, and role components to achieve its Strategic Goals, Objectives, and Services.

Security Architecture Management

The practice and process to articulate and model a full security architecture mapped to the Business, Strategy, Data and Information, Services, Application and Technology architecture. The security architecture should be lined and cross-mapped with the other layers and dimensions to show different levels of security points in the pre-existing developments. By Managing this capability, entities would be able to detect different types of functional and technical vulnerabilities in their exact location.

Security Standard

Define the baseline standard architecture of the security wherein it should show the security measurement and controls in each layer, for example, in the business layer, in the strategy layer, in the technology layer, etc. Each control type is defined based on each vulnerability type and the associated risk scenario.

Security Product Roadmap

Security Architecture and Security Standards will be the foundational components of planning, designing, acquiring, and implementing any business, functional, or security products.

EA Pre-requisites (Technology, Process, People)

- Define or choose a proper EA framework that covers the requirements of the entity industry and/or components.
- Select representation language to be used in conducting the various models with clear predefined metamodels like ArchiMate.
- L Ř Ŝ y ű ǎ Ŧ è l · f f 9 y ű ǎ ű ǎ Ŝ ă Ω ō dz ă ǎ y ă Ŝ ă ǎ t standards.
- State all Regulatory and Governance compliance rules and regulations.
- Allocate and assign the trained resources and formulate the team that will be responsible for building, operating, and maintaining the enterprise architecture practices.

- Define the proper needed tech solution and tools to support all the EA processes and activities.
- Define all process owners and stakeholders.
- Identify the governance model, workflows, and the change management process.

The Benefits of Applying Enterprise Architecture Management

Incorporating this capability within entities will yield a multitude of benefits, such as:

- Provide and maintain a Holistic View of the Business Dimensions and Artifacts.
- Detect business, strategy, functional, and technology deficiencies and vulnerabilities in different business dimensions and levels.
- Develop integrated Digital and Cybersecurity strategies.
- Build the Zero-Trust architecture mapped with comprehensive business models at different levels.
- Construct a suitable cybersecurity architecture in reference to different business risk seniors and integrate Key Risk Indicators into Key Performance Indicators.

1.3 Portfolio Management

Portfolio management in security is the process of carefully selecting and managing a group of investments to achieve specific business objectives while considering the investor's risk tolerance. This involves selecting suitable investments based on goals, timelines, and risk tolerance, monitoring them over time, and making necessary adjustments as required.

The term also refers to an entity's ability to efficiently manage a collection of initiatives, projects, and programs to achieve strategic objectives. In other words, it is a way to bridge the gap between strategy and implementation. Senior leadership plays a crucial role in executing the strategy, maximizing business value delivery, and safeguarding the portfolio's value through continuous monitoring and evaluation.

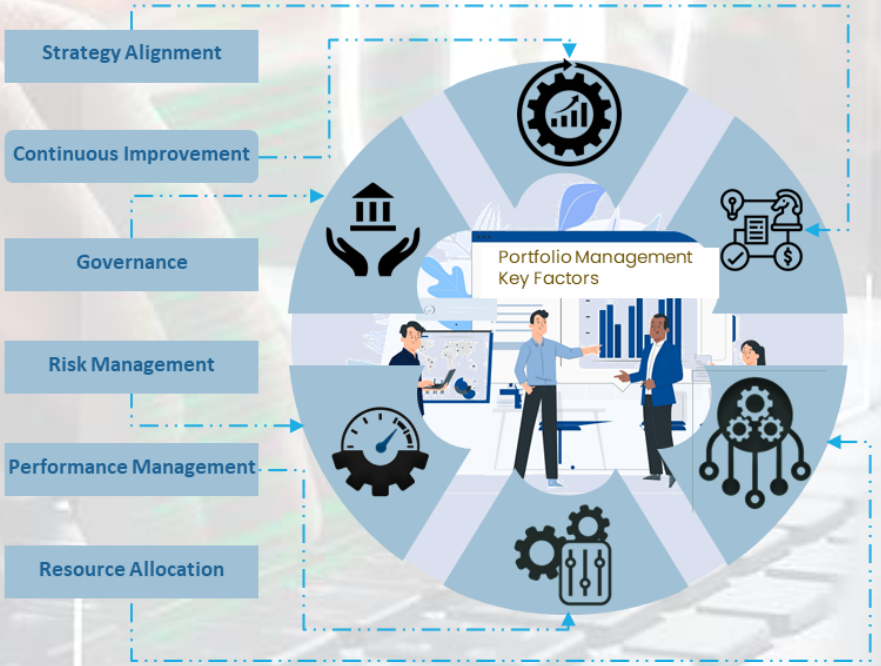
In the context of cybersecurity, portfolio management capability involves managing a portfolio of cybersecurity initiatives to improve the entity's overall security posture. The process includes:

- Defining business objectives.
- Inventorying projects and requests.
- Prioritizing projects, Validating project feasibility, Managing and monitoring the portfolio.
- Making trade-off decisions to maintain alignment with strategy and execution.

Portfolio Management Key Factors

A mature portfolio management capability includes several key elements:

- **Governance:** A clear and effective governance framework that defines roles, responsibilities, and decision-making processes for managing the cybersecurity portfolio.
- **Strategy Alignment:** A strong alignment between the cybersecurity portfolio and the entity's overall business strategy, goals, and objectives.
- **Risk Management:** An effective risk management process that identifies, prioritizes, and mitigates cybersecurity risks in the overall business risk landscape context.
- **Resource Allocation:** A process for allocating resources, including personnel, funding, and technology, to cybersecurity initiatives based on their priority and potential impact.
- **Performance Management:** A system for monitoring and reporting on the performance of the cybersecurity portfolio, including progress toward strategic objectives and return on investment.
- **Continuous Improvement:** A culture of continuous improvement that fosters innovation, collaboration, and learning from past experiences.



Overall, Portfolio management capability requires a clear understanding of long-term goals, risk tolerance, and investment options, as well as the ability to

weigh strengths and weaknesses, opportunities, and threats across the full spectrum of investments.

Security Initiatives Epics /Security Plan

To implement Portfolio Management properly, capturing and maintaining security initiatives Epics/Security Plan capabilities is important. These initiatives refer to a large body of work related to security that is broken down into smaller stories and managed within the context of a larger security initiative. Security initiatives may focus on specific areas like Process Solidification, Awareness, Capacity Building, Data and Information Identification and Security, Service Resiliency, Network security, or access management. Each of these components should be further broken down into stories that can be completed within a short period of time. This approach helps entities manage security risks effectively by prioritizing initiatives that align with their overall security goals and breaking them down into smaller, more manageable chunks of work.

To develop a security plan, entities should create security initiatives that align with their overall security goals. A security plan should typically include a description of the entity's security objectives, a risk assessment and measurement that identifies threats and vulnerabilities, and a set of controls and procedures for mitigating those risks.

Portfolio Management Pre-requisites (Process, People)

Effective portfolio management capability requires the right combination of people and processes. Below are the key pre-requisites in each of these areas:

- People:
  - Governance structure: A well-defined governance structure with clearly defined roles and responsibilities for managing the cybersecurity portfolio.
  - Expertise: A team with expertise in cybersecurity, risk management, project management, and business strategy.
  - Collaboration: A culture of collaboration and communication between cybersecurity teams and other stakeholders in the entity, such as IT, legal, compliance, and business units.
- Process
  - Strategy alignment: A process for aligning the cybersecurity portfolio with the entity's overall business strategy, goals, and objectives.
  - Enterprise Architecture: A well-established Enterprise Architecture practice.
  - Risk management: A process for identifying, prioritizing, and mitigating cybersecurity risks in the overall business risk landscape context
  - Resource allocation: A process for allocating resources, including personnel, funding, and technology, to cybersecurity initiatives based on their priority and potential impact.
  - Performance management: A system for monitoring and reporting on the performance of the cybersecurity portfolio, including progress toward strategic objectives and return on investment.

Effective portfolio management capability requires a balance between these prerequisites. The right combination of people and processes can help entities

effectively manage their cybersecurity portfolio, prioritize their efforts and resources, and improve their overall security posture.

The Benefits of Applying the Portfolio Management Capability

Incorporating this capability within entities will yield a multitude of benefits, such as:

- **Inistitunalize Cyber Security Economics** Portfolio management enables entities to prioritize and manage risks related to cybersecurity more effectively by identifying and economically addressing the most critical business risks first.
- **Improved Decision-Making** Entities can make more informed decisions about cybersecurity investments and prioritize initiatives aligning with their security goals and objectives using a portfolio management approach.
- **Resource Optimization** Portfolio management will help entities allocate resources more efficiently by identifying areas where investments can significantly impact cybersecurity.
- **Enhanced Visibility** Portfolio management provides a holistic view of the entity's cybersecurity posture, enabling stakeholders to make more informed decisions about cybersecurity risks and investments.

1.4 Service Product Portfolio

A service product portfolio in cybersecurity is a practice of managing the services Produced or to be produced to secure an entity's services and data from cyber-attacks. These services could be technologies or services acquired, outsourced, developed, or enhanced to achieve the cyber security strategic goals

To be effective in terms of cybersecurity, a service product portfolio should comprise a variety of services tailored to address various areas of cybersecurity. Services that focus on people, processes, and technology, such as:

- People: Services focused on people may include training and awareness programs that help employe understand and mitigate cyber risks. This could inclu training on topics such as password security, phishi attacks, social engineering, cyber security trends, etc.

- Process: Services that are focused on the process may include services that help entities develop and implement effective cybersecurity policies and procedures. This could include services that he entities to conduct risk assessments and measurements, implement security controls, and respond to potential security incidents.

- Technology: Services that are focused on technology may include services that help entities implement and manage cybersecurity technologies, such as firewalls, intrusion detection systems, encryption and vulnerability management. This could include services that help entities to assess their technology needs and select the most appropriate solutions.

The capability of a service product portfolio refers to the entity's ability to track and monitor the effectiveness of the products and services selected to fulfill the initiatives designed and approved in the cyber security portfolio. This can include the availability of resources such as qualified staff and equipment and the ability to respond to changing environment, culture, technology needs, and market conditions. Overall, a well-developed service product portfolio and strong capabilities will help entities track and monitor the effectiveness of the products and services to fulfill the objectives designed or procured.

- A security products and services catalog is a document that lists all of the security products and services that an entity outsourced, administers, manages, develops, or acquires. Security cameras, alarms, access control systems, software and hardware solutions, security learning management systems, and security consulting services are examples of such products and services. Each product or service is often described in full in the catalog, including functions, features, specifications, human resources, continued effectiveness and efficiency evaluation, pricing, and ROI analysis

- Security classifications of the services and products listed, tracked, and monitored in the service product portfolio categorize them based on their level of sensitivity and the potential impact of implementing them. The specific security classifications used by an entity may vary Each product or service may have its own security classification depending on its potential impact and the level of protection it provides. For example, a security camera system may be classified as unclassified, while a biometric access control system may be classified as confidential or secret. It is important for entities to consider the security classifications of their products and services carefully and ensure that they provide the appropriate level of protection.

- Security reviews can be used to assess the security of each product or service in the catalogue. This can help the entity identify potential

vulnerabilities and risks affecting the objectives and take steps to address them.

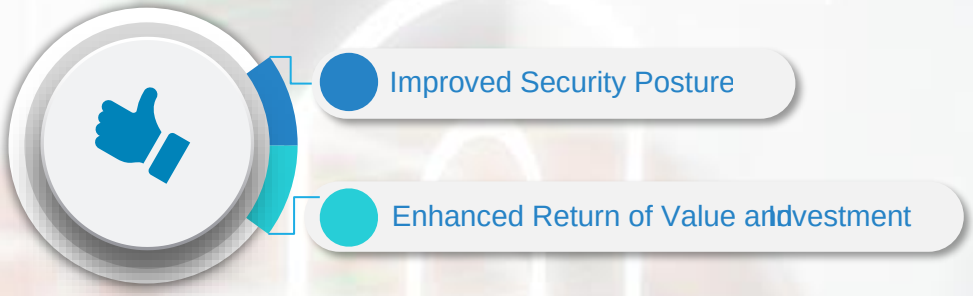
- TLM (Technology Lifecycle Management) is a comprehensive strategy for managing an entity's products and services throughout its lifecycle. It assists in planning, acquiring, deploying, maintaining, and retiring products and services in order to maximize their value while minimizing costs. TLM is based on a comprehensive perspective of the full technology service process lifecycle, considering asset utilization, qualification, skills, cost, and compliance. TLM also assists entities in more effectively and efficiently managing their products and services by offering visibility into their resources and assets, enabling proactive decision-making, and helping entities to understand and maximize the value of their investments and identify possible cost savings areas.

Service Product Portfolio Prerequisites (Technology, Process, People)

- Technology: Entities might consider enterprise solutions to track, monitor, and provide functional and financial analysis of the effectiveness, efficiency, utilization, SLAs, human resources capabilities, and response of the services or products implemented.
- Processes: entities must have well-defined processes in place to track, monitor, and manage products and services.
- People: entities must have the necessary staff with the necessary skills, qualifications, and knowledge to track, monitor, and manage products and services implemented.

Service Product Portfolio Benefits:

From a cybersecurity perspective, there are advantages and disadvantages to the product and service portfolio.



- Improved Security Posture: Entities will be able to continuously manage products and services implemented to improve their overall security posture and prevent or mitigate future security incidents.
- Enhanced Return of Value and Invencement: Entities will be able to practice and economically measure the effectiveness of the services and products introduced as controls to mitigate specific risk scenarios.

2 Security in Development

The measure and technique used during the service development process to ensure that the resulting system is secure and protected against potential threats and vulnerabilities. This includes practices such as vulnerability assessments, security testing, and adherence to industry-standard security protocols and guidelines.

Furthermore, it entails involving security experts and stakeholders throughout the development process to ensure that security considerations are incorporated into each phase of service or software development. Security in development is critical for protecting sensitive information and maintaining system integrity.

To have this consolidating capability, the following nine capabilities which are called Requirements to Deploy Functions must be developed, maintained, and activated within the entity as an entity or an individual with the appropriate maturity level:

1. **Requirements Management Capability** The ability to gather, document, and manage the requirements of the software system, including gathering input from stakeholders and ensuring that the software system meets the needs of users.

2. **Product & Team Backlog Capability** The ability to maintain and prioritize a backlog of requirements, features, and user stories that need to be implemented. This helps to ensure that the software system is aligned with the needs of stakeholders.

3. **Service/ product Design Capability** The ability to design and plan the architecture, layout, and overall design of the software system. This includes creating detailed plans and specifications and ensuring that the software system is aligned with IT as well as cybersecurity governance best practices.

4. **Secure Code Management Capability** the ability to implement secure coding practices, such as input validation, error handling, and secure data storage, to help prevent common software vulnerabilities. This includes using secure coding standards, such as OWASP Top 10, and following best practices for software development.

5. **Test Management Capability** the ability to use automated testing tools, such as unit tests, integration tests, and regression tests, to ensure that the software system is functioning correctly and is free of bugs or errors. This includes implementing automated testing and penetration testing as part of the CI/CD pipeline to ensure that the software system is secure and meets the requirements of stakeholders.

6. **CI/CD Pipeline Capability** the ability to implement a CI/CD pipeline to automate the software development process, including automated testing, building, and deployment. This includes integrating security testing into the CI/CD pipeline to ensure that new code changes do not introduce any vulnerabilities or security issues.

7. **Defect Management Capability:** Security in development is the process of identifying, tracking, and resolving security-related defects in the software system. It includes capabilities such as security defect tracking, resolution, root cause analysis, reporting, and vulnerability management.

8. **Build Management Capability:** The ability to manage the build process, including version control, testing, and packaging of software systems. This includes automating the build process, managing dependencies, and ensuring that the software system is ready for deployment.

9. **Release Management Capability:** The ability to plan, organize, and manage the release of software systems, including testing, packaging, and deployment. This includes identifying the appropriate release schedule, determining the release criteria, and coordinating the release process with stakeholders.

A Comprehensive Overview

The following exposition provides a comprehensive overview of this main capability and its sub-capabilities among its counterparts to provide a detailed analysis of the capability and its components. By minding this capability and its sub-capabilities, entities can gain insights into how they interact and utilize it to achieve the desired outcomes according to their field and business requirements. This overview is intended to serve as a valuable reference for understanding this critical capability.

2.1 Requirements Management Capability

Requirements Management is a critical component of any development process. It involves identifying and documenting the needs and expectations of stakeholders, such as users and customers, and defining the software to be developed LJ 2 NJ Ř specific requirements to satisfy those needs and expectations.

The goal of requirements management is to ensure that the software, hardware, soluitons and/or services being developed is aligned with the needs and expectations of stakeholders and that it is developed per the overall project objectives. This typically involves identifying the requirements of the product, documenting those requirements clearly and concisely, and tracking the progress of the development against those requirements.

Requirements management in cyber security is critical to ensuring the security and integrity of a system and protecting its services and information from potential threats or vulnerabilities. Entities can effectively safeguard their systems and data and protect themselves from cyber attacks or breaches by properly managing security and privacy requirements.

Requirements Management Phases

Requirements management involves several phases, including requirements planning, elicitation, analysis, documentation, validation, and management.

- **Requirements Planning**: This involves defining the overall strategy for requirements management, including the roles and responsibilities of stakeholders, the methods, and tools to be used, and the approach to requirements elicitation, analysis, documentation, and validation.
- **w Ŝ lj dz ƛ NJ Ŝ Y Ŝ y ű Ω ă**: This involves gathering and identifying the requirements for the project or system. This may involve conducting interviews, surveys, workshops, or other techniques to gather input from stakeholders, such as the customer, the development team, and any other interested parties.
- **w Ŝ lj dz ƛ NJ Ŝ Y Ŝ y ű Ω ă**: This involves analyzing and organizing the requirements that have been gathered to identify any inconsistencies, ambiguities, or gaps. This may involve creating a requirements hierarchy or other visual representation of the requirements to help stakeholders understand and agree on the requirements.
- **w Ŝ lj dz ƛ NJ Ŝ Y Ŝ y ű Ω ă**: This involves documenting the requirements in a clear and concise manner, using a standardized format and language. The requirements document should include details such as the purpose, scope, and constraints of the project, as well as the specific requirements for each aspect of the system.
- **w Ŝ lj dz ƛ NJ Ŝ Y Ŝ y ű Ω ă**: This involves verifying and validating the requirements to ensure that they are complete, consistent, and accurate. This may involve reviewing the requirements with stakeholders, conducting testing or simulations, or using other methods to ensure that the requirements meet the users' or customers' needs.
- **w Ŝ lj dz ƛ NJ Ŝ Y Ŝ y ű Ω ă**: This involves tracking, managing, and controlling the requirements throughout the project. This may involve updating the requirements document as necessary, communicating changes to stakeholders, and managing any changes to the project scope or timeline.

Security & Privacy as a Principal for Requirements Management

Security and privacy are critical considerations in requirements management. Ensuring the security and privacy of the project's requirements is important to protect sensitive information and prevent unauthorized access to the project's data and resources.

It is important to identify and document these requirements clearly and accurately and to track and manage changes to them over time. It is also important to ensure that the requirements are consistently and effectively implemented in the system or application to ensure its security and protect sensitive information from potential threats or vulnerabilities.

- **Confidentiality**: Requirements should be kept confidential to prevent unauthorized access or disclosure.
- **Integrity**: Requirements should be protected from unauthorized modification or tampering to ensure their accuracy and reliability.
- **Availability**: Requirements should be readily accessible to authorized users to ensure that development can proceed efficiently and effectively.
- **Privacy**: Requirements may contain sensitive or personal information, and it is important to ensure that this information is protected from unauthorized access or disclosure.
- **Security**: Requirements should be protected from external threats such as hacking or malware attacks to ensure their integrity and reliability.
- **Compliance**: Requirements should be managed in a way that complies with relevant laws, regulations, and industry standards to ensure the security and privacy of the system being developed.

Requirements Management Prerequisites

The prerequisites for successful requirements management include the following:

- Requirements management tools are essential for effectively managing and tracking the requirements throughout the project. These tools should support the various requirements management activities such as elicitation, analysis, documentation, review, and approval.
- A well-defined and structured requirements management process is essential for ensuring that the requirements are accurately gathered, analyzed, documented, reviewed, and approved. This process should be documented in a requirements management plan and followed consistently throughout the project.
- A dedicated requirements management team with the appropriate skills and expertise is essential for successfully managing the requirements throughout the project. This team should include representatives from various stakeholder groups, subject matter experts, and project managers. Effective communication and collaboration among the team members are also essential for ensuring the requirements are accurately gathered, analyzed, documented, reviewed, and approved.

The Benefits of Applying the Requirement Management Capability

Incorporating this capability within entities will yield a multitude of benefits, such as:

- **Prioritize Requirements:** It helps to prioritize requirements, allowing the development team to focus on the most important and valuable features of the product or system.
- **Security Enhancements:** Clearly defined requirements guarantee that security requirements are explicitly included, so improving system security.
- **Development Aligned with Objectives:** Vulnerability risks are reduced when development activities are consistently aligned with requirements and compliance standards.
- **Mitigation of Potential Threats:** Explicitly addressing potential threats in requirements allows for proactive mitigation during development.
- **Regulatory Compliance:** Clear requirements articulate and ensure adherence to regulatory and compliance standards.
- **Efficient Resource Utilization:** Streamlined resource allocation focuses cybersecurity efforts on critical security needs.
- **Reduced Cybersecurity Incidents:** Thorough management of security requirements minimizes the risk of incidents and breaches.
- **Improved Incident Response:** Well-documented security requirements facilitate efficient incident response processes.
- **Enhanced Communication and Collaboration:** Clear requirements foster collaboration and a shared understanding among development teams, cybersecurity professionals, and stakeholders.
- **Cost Reduction:** Addressing security requirements early prevents costly rework and modifications later in the process.

3. **Continuous Improvement:** Requirements management establishes a framework for ongoing assessment and improvement of cybersecurity measures.

2.2 Product & Team Backlog Capability

A product backlog is a prioritized list of tasks that must be completed in order for a product to be developed and launched successfully. It often comprises user stories as well as additional items required to construct the product, such as technical or design activities. The product owner owns the product backlog, which is utilized by the development team to plan and execute the work required to construct the product.

A team backlog is similar to a product backlog, but it is specific to one development team rather than the entire product. It covers the work that the team has committed to completing in a given sprint, as well as any additional items that the team may need to work on to support the product backlog. The development team owns the team backlog, which is used to plan and track the team's progress on the work they have agreed to do.

A product backlog's and a team backlog's capabilities are directly tied to their ability to give a clear and actionable plan for the development team. This means that the items on the backlog should be specific and detailed enough for the team to comprehend what needs to be done. Furthermore, the backlog items should be prioritized so that the team may focus on the most important tasks first.

A well-managed product and team backlog should also be adaptable, allowing the team to revise their plans as needed in reaction to changes in the product or development process. This can be accomplished by reviewing and refining the backlog on a regular basis to ensure that it appropriately reflects the current status of the product and the team's priorities.

Overall, the capability of a product and team backlog is determined by their ability to support the team in their work and help them to effectively deliver high-quality products.

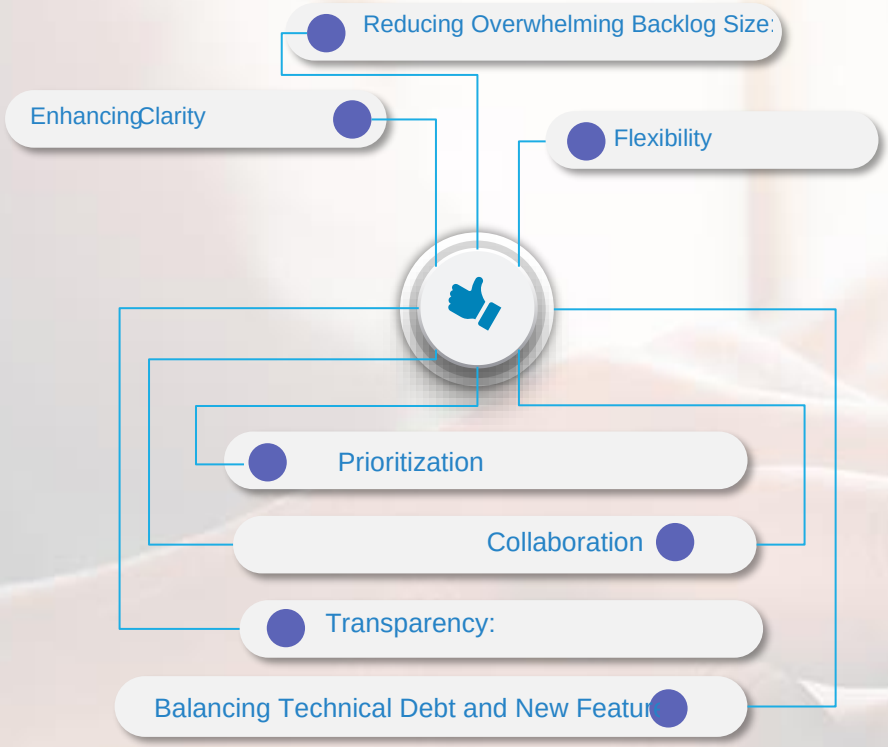
Product & Team Backlog Pre-requisites (Technology, Process, People)

The prerequisites for a product and team backlog to be effective include the following:

- **Technology**: The team will need access to a project management tool that allows them to create and manage the backlog. This could be a tool specifically designed for agile project management or a more general purpose tool that allows the team to create and prioritize items on the backlog.
- **Process**: The team will need to have a clear understanding of the agile development process and be committed to using agile principles and practices to manage their work. This includes a clear understanding of the role of the product owner and the development team, as well as the principles of sprint planning, daily stand-up meetings, and sprint retrospectives.
- **People**: The team will need to have a mix of skills and expertise to support the development process. This includes having a product owner who is responsible for managing the product backlog and ensuring that it accurately reflects the priorities of the business, as well as having a development team with the technical skills and experience to build the product effectively.

The Benefits of Product and Team Backlog Capability

Incorporating this capability within entities will yield a multitude of benefits, such as:

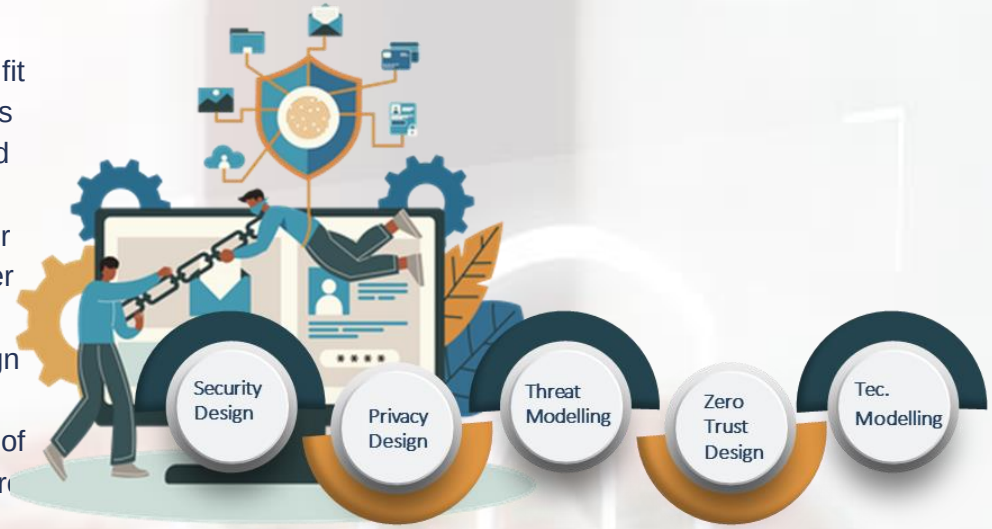


- **Prioritization:** A well-maintained product backlog helps prioritize cybersecurity tasks based on their significance and potential impact. It allows the team to focus on the most critical vulnerabilities and risks first, ensuring that limited resources are allocated effectively.
- **Transparency:** The backlog provides transparency into the cybersecurity initiatives and tasks being worked on. It enables stakeholders, including management and clients, to have visibility into the team's progress, understand the security priorities, and make informed decisions.
- **Collaboration:** A backlog promotes collaboration among team members. It serves as a centralized repository of tasks, allowing team members to have a shared understanding of what needs to be done. It encourages cross-functional collaboration and coordination, which is crucial in cybersecurity to address diverse threats and vulnerabilities.
- **Flexibility:** Backlogs can be adjusted and reprioritized as new threats or vulnerabilities emerge. This flexibility enables the team to adapt to evolving security challenges promptly and make necessary adjustments to their plans and priorities.
- **Reducing Overwhelming Backlog Size:** If the backlog becomes too large or poorly managed, it can become overwhelming for the team. This can lead to inefficiencies, confusion, and difficulty in identifying the most critical tasks. It is essential to maintain a manageable backlog size by regularly reviewing and refining it.
- **Enhancing Clarity:** Backlog items should be well-defined and include clear acceptance criteria to avoid ambiguity. In cybersecurity, where precision is vital, vague or incomplete backlog items can hinder the team's progress and result in miscommunication or misunderstandings.
- **Balancing Technical Debt and New Features:** In cybersecurity, addressing technical debt (existing vulnerabilities and weaknesses) alongside new feature development is crucial. However, balancing these competing priorities in the backlog can be challenging. Failure to allocate sufficient time and resources to address technical debt can result in increased cybersecurity risks over time.

Overall, when effectively managed and maintained, product and team backlogs can provide numerous advantages in the realm of cybersecurity. However, it is important to address potential challenges and risks to ensure that the backlog remains a valuable tool for the team's security initiatives.

2.3 Service / Product Design Capability

Service design practice is to create products and services that are holistically fit for purpose, meaning they meet the needs and expectations of the customers internally or externally, and optimally fit for use, meaning they can be delivered effectively by the entity and its ecosystem. This includes considering the technical requirements of the products and services and optimizing customer experience (UX) along the designed customer journey with all optimal user interfaces (UI) and the business processes needed to deliver them. In the context of cybersecurity, the design should take care of all security by design principles and guidelines in reference to the entity business transformation security strategy, regardless of the design phase. This required the execution of each subfield of the designing capability as below. Where the goal is to ensure a highly secure product or service with less / minimum vulnerability to cyber or security breaches, the Designing practice optimally goes in different phases and links with other capabilities mentioned in this framework; additional information to elucidate this in the SPD dependency section. In general, the design will go like the below diagram with capsulation of the security aspect :



- **Security Design**

  The present holistic security design is characterized by its continuous and horizontal integration with each phase of the overall design practice. Its primary objective is to guarantee that security checkpoints are identified for each component type, such as data processing aspect, infrastructure, etc. Each security checkpoint is designed to address distinct security issues and types, such as confidentiality, integrity, and availability (CIA).

  It is imperative to continuously monitor and manage the security design, especially when changes are being generated and adapted. The process of security design is central to safeguarding sensitive data and assets. Therefore, it involves regular reviews and updates of security measures to protect against the latest threats and vulnerabilities.

  In conclusion, the holistic security design is a fundamental aspect of any business or academic setting. Its purpose is to ensure the apprehension of security checkpoints in each phase of the design process and to address different security issues and types while continuously monitoring and managing the security design. Regular review and updates of security measures are essential to maintaining the confidentiality, integrity, and availability (CIA) of sensitive data and assets.

- **Privacy Design**
  Privacy design represents a fundamental element of security that aims to guarantee efficient accessibility mechanisms to the right individuals whilst properly preserving personal data. The design of effective privacy solutions within the context of cybersecurity involves considering potential risks and vulnerabilities that may compromise user data and implementing measures to mitigate such risks. This comprises the careful determination of the appropriate levels of authentication and encryption, as well as the development of policies for privacy use management. It is of utmost importance to ensure that such procedures enable the optimal protection of personal data by regulating its collection, storage, processing, and sharing whilst adhering to applicable legal and regulatory frameworks.

- **Threat Modelling**
  Threat Modelling is a process that involves creating models that act as testing scenarios of various potential threats that may affect the different assets related to the product or service. This process considers the full journey of the customers and touchpoints. Each potential threat must be defined, modeled, and analyzed alongside the associated assets for frequency, capability, and loss magnitude

- **Zero Trust Design**
  Zero trust design is a security approach that adheres to the "never trust, always verify" philosophy. It is a preventative technique that treats all identities as untrusted unless proven otherwise. This means that there should be no implicit trust between any user, device, or agent. Instead, any attempt to access entity resources must demonstrate its reliability. This applies to all devices and systems. Zero trust design aims to provide secure access for users, devices, and applications across networks and clouds without compromising user experience, and it is crucial to design the verification of trustworthiness based on the nature of the product or service. Therefore, implementing zero-trust design requires developing an appropriate environment based on the product or service in order to build a secure infrastructure.

- **Technology Modelling**
  This is the tech-design part of the overall design capabilities that address and support making the right technology requirement for the right functionality, including all supporting components in capsulation with the security designed level. It should determine the appropriate security measures and technologies needed to protect against potential cyber threats and any necessary infrastructure or support systems. This may involve conducting security assessments, penetration testing, and implementing measures to protect against data breaches and other cyber attacks.
  Testing and prototyping, like the pilot phase or POV, are highly recommended tech-design methodologies that ensure the effectiveness and optimization of technology services. This part is linked with EA technology architecture modeling.

Service Product Design Pre-Requisites (Technology, Process, People)

Pre-foundational elements or practices should be at least maintained in regard to proper and effective service product design practice and from the process, people, and technology perspectives:

- **Process** Well-established, Predefined, and Approved designing process, which identifies roles and responsibilities and steering committee's role for approvals and change management.
- **People** Defined and assigned qualified and skilled resources with clear roles and responsibilities for each design phase
- **Technologies and Tools** Different tools might be introduced as needed to model, design, review, and simulate different scenarios related to products

or components of the product for analyzing threats and vulnerabilities to reduce cyber security attacks and impact.

The Benefits of Applying the Service Product Design Capability

Incorporating this capability within entities will yield a multitude of benefits, such as:

- Develop products/services with minimal vulnerabilities: Ensure the development of a product or service with minimal vulnerabilities throughout the entire user experience (UX) and user interfaces (UI) while optimizing security through design features
- Ensure the development of the required level of prevention and security aligned with business, cyber risk, and zero trust strategies.
- Maintain the scalability possibility of maintaining performance along security and cybersecurity standards
- Manage cost effectively and in an optimized way according to the suitable security and risk mitigation designed plans
- Define possible and optimal checkpoints for continuous penetration testing.
- Optimize the utilization of other related capabilities that enhance the security of the product or service as the design plays a managerial role for them (Secure Code Management, Test Management, CI/CD Pipeline, Build Managing, and Release Management)

2.4 Secure Code Management Capability

Developing computer software involves several stages, one of which is secure coding. It is a practice that aims to prevent the accidental introduction of security vulnerabilities into the code. It encompasses the disciplined creation, storage, version control, and distribution of code while prioritizing security measures throughout the software development lifecycle. By implementing stringent access controls, encryption protocols, and vulnerability assessments, secure code management mitigates risks posed by potential exploits, breaches, or unauthorized access.

In addition, modern cryptographic algorithms can be used to encrypt data, which increases the security of the code in case of a breach. Secure key management best practices should also be followed.

To identify security-related weaknesses in an application's source code, a secure code review is necessary. This specialized task involves a manual and/or automated review of the code.

- **Code Quality Management:** Code quality management is the process of ensuring that the source code of a software application is well written, maintainable, and reliable through:
  - Write code that follows best practices and coding standards and conduct code reviews to identify and fix issues.
  - Automating testing to ensure that code changes do not break existing functionality.
  - Using tools to analyze code for security vulnerabilities or performance problems.

- **Peer Review:** Peer review is a process in which code is reviewed by one or more colleagues familiar with the programming language and platform. Peer review is often used as a quality assurance measure to ensure that code is high quality and adheres to established standards and guidelines.

- **Security Static Code Analysis:** Security static code analysis is analyzing source code for security vulnerabilities and issues. It is called "static" because it is performed on the code itself rather than on the code as it is running. Static code analysis for security involves examining the source code to detect potential vulnerabilities and problems.

Secure Code Management Pre-requisites (Technology, Process, People)

Several key prerequisites for effective Risk and Compliance Management include technology, process, and people.

- **Technology:**
  - **Version Control Tools** helps manage code changes over time, allowing multiple developers to work on the same codebase simultaneously and keep track of each change. Identify all entities' business Policies, procedures, and business rules and standards.
  - **Automated testing Tools:** helps automatically test code for vulnerabilities, such as static code analysis tools or dynamic testing tools.
- **People:**
  - **Security Training for Developers:** It's important for developers to understand how to write secure code and to be aware of common vulnerabilities and how to prevent them.
- **Process:**
  - **Access Controls:** It's important to have controls in place to ensure that only authorized individuals have access to the codebase and to ensure that changes to the code are made by authorized individuals.
  - **Secure Code Review:** Establishing a secure code review process is crucial for ensuring that code changes are reviewed by other

developers before they are deployed. This can help catch security vulnerabilities and other issues before they reach production.

The Benefits of Applying the Secure Code Management Capability

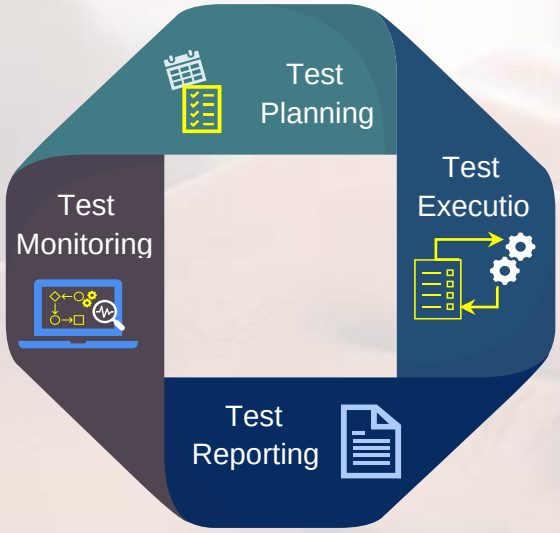
Incorporating this capability within entities will yield a multitude of benefits, such as:

- **Improved security:** identifying and addressing vulnerabilities in code, preventing security breaches, and protecting sensitive data.
- **Increased Trust:** Mature code capabilities increase trust in product and service security.
- **Enhanced Compliance:** ensure that products and services meet industry standards and regulatory requirements.
- **Improved quality:** reduce the number of defects and errors.

2.5 Test Management Capability

Test management capability is an essential process in cybersecurity that involves planning, executing, and monitoring various tests and scans to ensure a system's or network's security and resilience. This process includes a broad range of activities, such as vulnerability scanning, penetration testing, and other types of testing, which help identify and mitigate security risks. The primary purpose of test management is to provide a comprehensive and structured approach to testing that enables entities to achieve their security goals cost-effectively.

The process of test management comprises several stages.



The first stage is test planning, which involves setting specific goals and objectives for the tests, defining the scope and coverage, identifying the necessary resources and personnel, and creating a schedule for the testing activities. It is crucial to define the scope of testing to ensure that all requirements are met and that testing is conducted efficiently and effectively.

The second stage is test execution, where the actual tests are conducted using various tools and techniques to evaluate the security of the system or network. This can include both manual and automated testing using specialized software.

The third stage is testing reporting, which involves documenting the results of the tests and providing recommendations for remediation or improvement based on the findings. The report should clearly outline any vulnerabilities or weaknesses that were identified, as well as any recommendations for addressing them.

The final stage is testing monitoring and control, which involves tracking the progress of testing and making necessary adjustments to ensure effective and efficient testing. It also involves managing and tracking any issues or risks that may arise during the testing process.

Security Testing

The security testing process assesses and identifies vulnerabilities and security flaws in an information system that attackers can exploit. It can be performed manually or through automation. The most common types of security tests include penetration testing and vulnerability scanning.

When security testing is done manually, the test management is responsible for ensuring that the suitable systems are tested with the appropriate tests at

the right time. This involves identifying which systems need to be tested, selecting the appropriate tests, and scheduling the tests. The test management also needs to keep track of the results of the security testing so that any problems can be addressed quickly.

When security testing is done automatically, the test management is responsible for configuring the tool and creating the environment in which the tests will be run. This includes installing and configuring the tool, setting up accounts and permissions, and ensuring that all necessary data is available to the tool. The test management also needs to monitor the progress of security testing and review the results to ensure that no issues have been overlooked.

Penetration Testing

Penetration testing should be an ongoing process as part of the entity's overall security strategy. By regularly testing systems, entities can stay one step ahead of the attackers and ensure that their defenses are up to date.

Before commencing any penetration test, it's important to identify and understand the objectives and expectations. Once all testing has been completed, it's critical to report on findings and recommendations. This report should be clear and concise, highlighting any critical issues that were identified during the engagement. Providing guidance on how these issues can be remediated is also important.

Vulnerability Scanning

Vulnerability scanning is a process of identifying potential security weaknesses in systems and software. A vulnerability scanner can be used to identify known vulnerabilities. Entities should run vulnerability scans on a regular basis, both internally and externally. External scans can be used to find vulnerabilities that attackers from the outside may exploit, while internal scans can find weaknesses that malicious insiders could exploit.

Vulnerability scanning needs to be used as part of a security assessment in order to identify areas where a system may be vulnerable to attack. It is also used on an ongoing basis in order to monitor for new or emerging threats.

Test Data Management and Data Anonymization

Test data management refers to the process of creating, organizing, and maintaining data that is used for testing software, systems, and processes. It involves several activities, such as creating test data sets, selecting the appropriate data for testing, storing and managing test data, and documenting it.

Data anonymization, on the other hand, is the process of removing or obscuring sensitive or personal information from data sets to protect individuals' privacy. This may involve removing or masking names, addresses, social security numbers, and other personally identifiable information.

Test data management and data anonymization are interrelated because test data may contain sensitive or personal information that needs to be anonymized to comply with privacy regulations. For instance, an entity may have a database of citizen records that it uses for testing purposes, and it may need to anonymize the data to protect individuals' privacy. In such cases, data anonymization techniques are used to remove or obscure personal information from the test data before using it for testing.

Unit and Functional Testing

Unit testing is a specific type of testing used for assessing individual units or components of a software application. The process of unit testing involves isolating each unit or component from the rest of the application and testing it individually to ensure that it is functioning correctly. Typically, unit tests are automated and run frequently during the development process to detect defects at an early stage.

In contrast, functional testing is a broader type of testing that evaluates the overall functionality of a software application. It generally involves testing the

application as a whole to determine if it is functioning correctly and meeting the necessary requirements. Functional testing can include several different types of testing, such as integration testing, system testing, and acceptance testing.

APITesting

API security testing is a critical aspect of ensuring the security and integrity of applications, especially in the context of modern web and mobile applications that rely heavily on APIs (Application Programming Interfaces) to communicate and exchange dat API security testing helps identify and mitigate vulnerabilities and weaknesses in APIs that could be exploited by malicious actors.

Performance and Load Testing

Performance and load testing are two types of testing used to evaluate a software application's performance and scalability under different conditions. The primary objective of these tests is to identify any issues or bottlenecks that may affect the system's performance and to determine its capacity and scalability.

Performance testing is specifically designed to evaluate a system's speed, responsiveness, and stability under normal and peak usage conditions. Its primary focus is to measure the system's performance when subjected to a specific workload.

On the other hand, load testing is used to evaluate the behavior of a system under a specific workload by analyzing its performance and identifying any bottlenecks or issues that may arise under heavy load. The primary objective of load testing is to determine the maximum capacity of the system and its ability to handle heavy loads without any performance issues.

Test Management Prerequisites (Technology, Process, People)

- **People** skilled testers who are familiar with the testing tools, techniques and the testing processes.
- **Process** effective change and release processes
- **Technology** It's important to have a testing environment that is separate from the production environment. This will allow testers to conduct tests without affecting the live system.

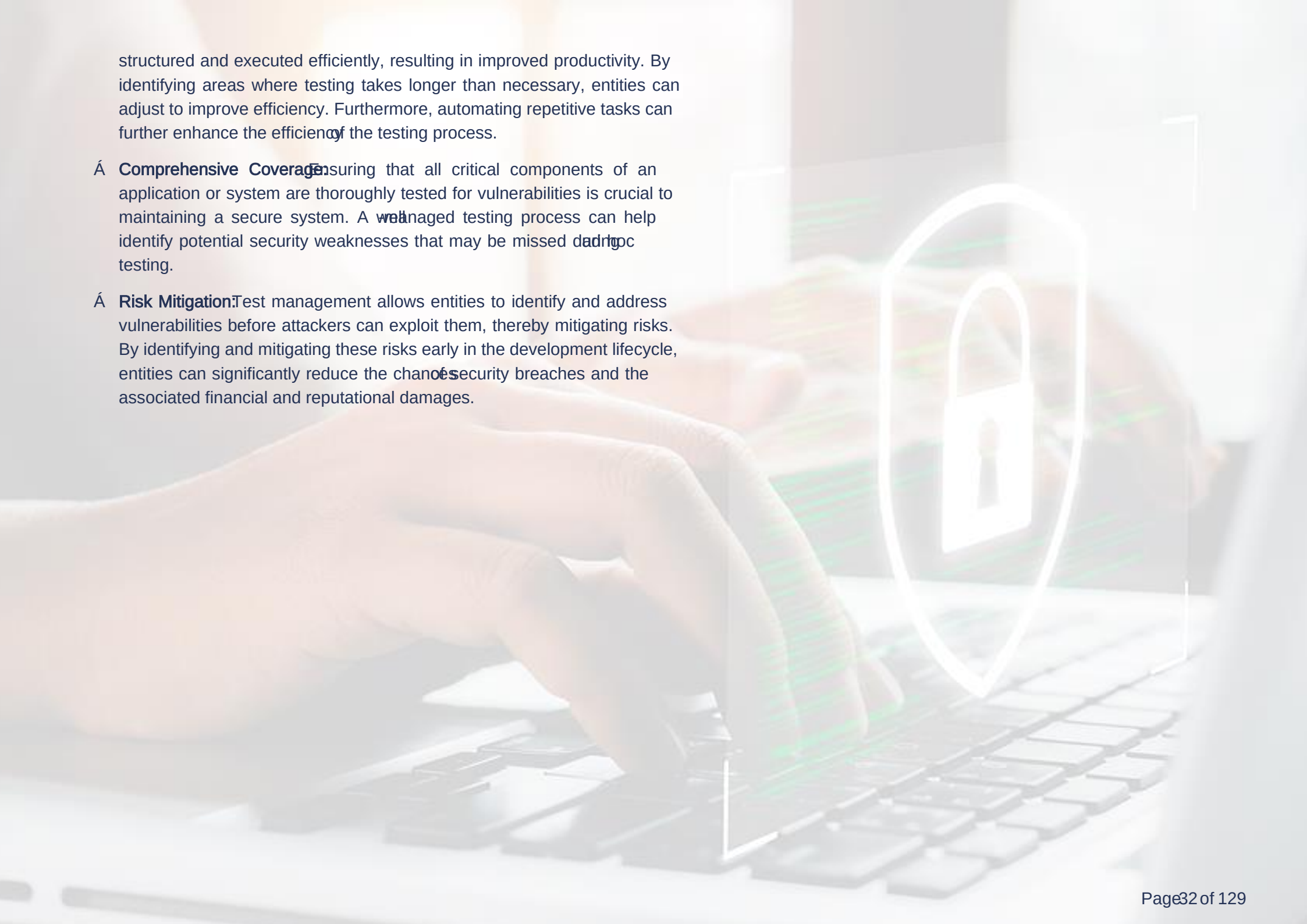
The Benefits of Applying the Test Management Capability

Incorporating this capability within entities will yield a multitude of benefits, such as:

- **Improved Quality** With a dedicated team responsible for managing testing, entities can ensure that their testing processes are on track and that quality standards are met. By conducting regular tests and tracking results, entities can identify and fix errors before they cause problems in production.
- **Increased Efficiency** Effective test management plays a vital role in reducing the time and cost of testing. It ensures that test plans are well

structured and executed efficiently, resulting in improved productivity. By identifying areas where testing takes longer than necessary, entities can adjust to improve efficiency. Furthermore, automating repetitive tasks can further enhance the efficiency of the testing process.

- **Comprehensive Coverage:** Ensuring that all critical components of an application or system are thoroughly tested for vulnerabilities is crucial to maintaining a secure system. A well-managed testing process can help identify potential security weaknesses that may be missed during ad-hoc testing.
- **Risk Mitigation:** Test management allows entities to identify and address vulnerabilities before attackers can exploit them, thereby mitigating risks. By identifying and mitigating these risks early in the development lifecycle, entities can significantly reduce the chances of security breaches and the associated financial and reputational damages.



2.6 CI/CD Pipeline Capability

Continuous Integration / Continuous Deployment (CI/CD) Pipeline Capability

Continuous Integration/Continuous Deployment is a software development practice in which code changes are automatically built, tested, and deployed to production. The goal of CI/CD is to enable teams to release software updates more frequently, with fewer errors, and with less effort. As a result, code releases can happen more often and with fewer bugs and security vulnerabilities.

CI/CD practices form the backbone of modern DevOps processes and allow DevOps teams to deliver code updates frequently, reliably, and quickly

Because of the similarity in terminology related to the (CI/CD) Pipeline, the following is an explanation of the abbreviations and their meanings:

- **Continuous Integration (CI):** Response to changes in source code, automatically pulling from version control and running a build process, which usually consists of verifying that unit and integration tests and other QA checks pass.

- **Continuous Delivery (CD):** Deploys passing builds to a staging environment, where further checks can be done to verify the behavior.

- **C (CD):** Automatically deploys to a production environment after staging checks have passed instead of needing manual approval.

Cybersecurity is an important consideration in the design and implementation of a CI/CD pipeline. This includes measures to protect the pipeline infrastructure and the code being built, tested, and deployed.

Securing CICD Pipeline as a Principal for CICD Pipeline

A secure CI/CD pipeline helps to protect against the introduction of vulnerabilities and malware into the software being developed and deployed. This is especially important for entities that handle sensitive data or operate in regulated industries, as a security breach could have serious consequences. In addition, a secure CI/CD pipeline can help entities maintain the integrity and reliability of their software. If the pipeline is not adequately secured, it could be vulnerable to tampering or attacks that could disrupt the development and deployment process. This could result in delays or disruptions to the software development lifecycle and ultimately lead to reduced productivity and customer satisfaction.

Finally, a secure CI/CD pipeline helps to protect against reputational damage and legal liability. If an entity's software is found to have security vulnerabilities or is used to distribute malware, it could damage the entity's reputation and potentially lead to legal action.

There are several measures that entities need to consider to secure their CI/CD pipelines from a cyber security perspective. Some key strategies include:

- **Implementing strong access controls:** This includes measures such as multifactor authentication, role-based access controls, and regular password updates to ensure that only authorized users have access to the pipeline infrastructure and code.

- **Ensuring secure communication:** This can be achieved using secure protocols and encryption for data in transit and at rest.

- **Implementing secure coding practices:** This includes training developers on secure coding practices and using tools such as static code analysis to identify and fix vulnerabilities in the code.

- **Conducting thorough testing:** Entities should use a combination of automated testing and manual review to identify and fix security vulnerabilities in the code.

- **Continuous monitoring:** Entities should implement continuous monitoring of the pipeline and its components for security vulnerabilities and suspicious activity. This can include using tools such as log analysis and intrusion detection systems.

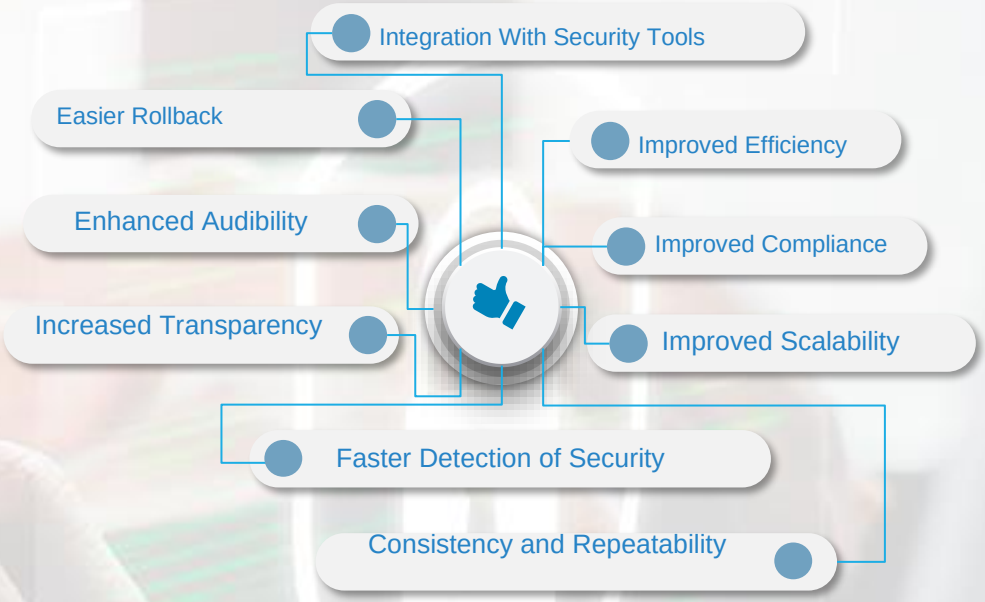
CI/CD Pipeline Capability Pre-requisites (Technology, Process, People)

There are several technology, process, and people pre-requisites for implementing a successful CI/CD pipeline:

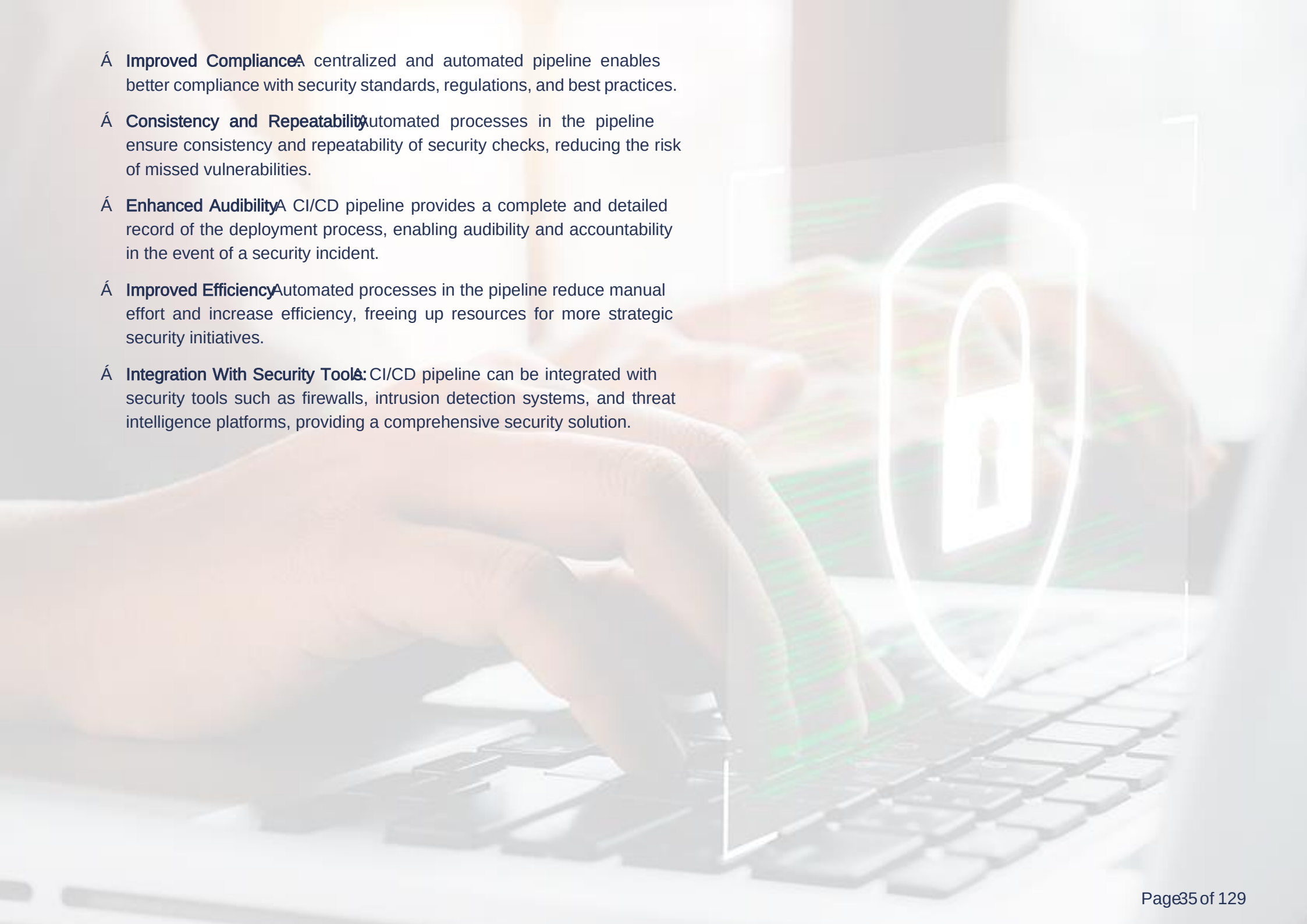
- **Technology:** Tools that might be used for monitoring, analyzing, and managing security in CI/CD.
- **Process:** A clear and defined process for managing code development, testing, and deployment. This should include defining roles and responsibilities, establishing coding standards and best practices, and setting up the necessary tooling and infrastructure to support the CI/CD pipeline.
- **People:** Skilled developers who are familiar with the tools and technologies used in the CI/CD pipeline and who are committed to following the established process for managing the codebase and dedicated DevOps engineers who are responsible for maintaining and optimizing the CI/CD pipeline and for ensuring that it runs smoothly and efficiently.

The Benefits of Applying the CI/CD Pipeline Capability

Incorporating this capability within entities will yield a multitude of benefits, such as:



- **Faster Detection of Security Issues:** With automatic testing and integration, security issues can be detected and addressed faster, reducing the risk of exploitation.
- **Easier Rollback:** With a CI/CD pipeline, it is easier to roll back to a previous version of the code in the event of a security issue, reducing the impact of a breach.
- **Increased Transparency:** A centralized pipeline provides better visibility into the deployment process, making it easier to identify and address security issues.
- **Improved Scalability:** A CI/CD pipeline enables systems to scale more easily, reducing the risk of security vulnerabilities as the systems grow and change.



- **Improved Compliance:** A centralized and automated pipeline enables better compliance with security standards, regulations, and best practices.
- **Consistency and Repeatability:** Automated processes in the pipeline ensure consistency and repeatability of security checks, reducing the risk of missed vulnerabilities.
- **Enhanced Audibility:** A CI/CD pipeline provides a complete and detailed record of the deployment process, enabling audibility and accountability in the event of a security incident.
- **Improved Efficiency:** Automated processes in the pipeline reduce manual effort and increase efficiency, freeing up resources for more strategic security initiatives.
- **Integration With Security Tools:** A CI/CD pipeline can be integrated with security tools such as firewalls, intrusion detection systems, and threat intelligence platforms, providing a comprehensive security solution.

2.7 Defect Management Capability

Any provided system could suffer from some defects, such as errors or flaws in the code, that can cause system problems or compromise functionality.

Defect management identifies, tracks, and resolves defects; the process involves identifying defects as early as possible in the development process, evaluating their impact and severity, and taking action to fix or mitigate them.

Effective defect management helps entities improve the quality and reliability of their systems, reduce the risk of defects being exploited by attackers, and improve customer satisfaction. To manage defects effectively, entities need to track and manage defects and establish clear processes for identifying, tracking, and resolving defects. It is also important to regularly review and update these processes to ensure that defects are effectively identified and resolved in a timely manner.

Defect management is an important aspect of cyber security that requires a systematic and proactive approach to identify, classify, and address vulnerabilities in computer systems, networks, and software. By implementing effective defect management process, entities can better protect themselves against potential cyber attacks and other threats. The following presents the vital phases of the Defect Management processes.

Identifying Defects

Identify defects as early as possible in the development lifecycle, typically through activities and tools and mechanisms such as threat modeling, vulnerability scanners, penetration testing, static analysis, and code reviews to identify vulnerabilities and weaknesses in a system.

Classifying Defects

Once defects have been identified, they must be classified according to their severity and impact on the system. This helps prioritize the defects that need to be addressed first.

Assessing Defects

The next step is to assess the defects to determine the risk they pose to the system. This may involve analyzing the likelihood of an exploit occurring, as well as the potential consequences if the defect is exploited.

Tracking Defects

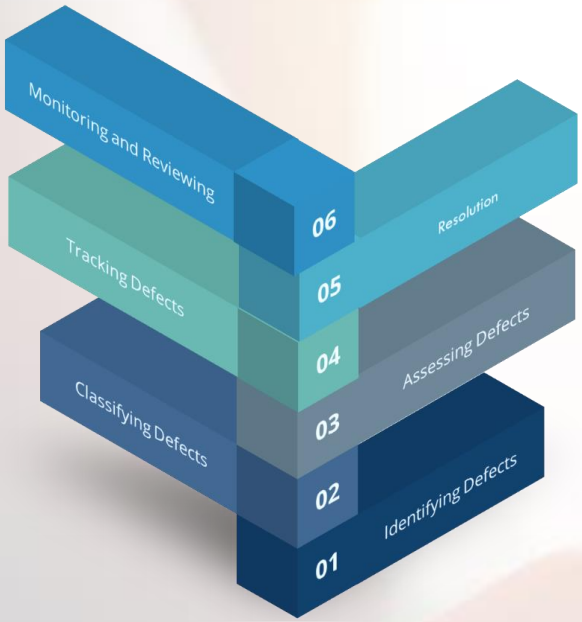
Maintaining a record of each defect, including its status, resolution, and any relevant information, such as test cases or code changes.

Resolution

Taking action to fix or mitigate defects may involve applying patches or updates, implementing additional security controls, redesigning the system to remove the vulnerability, repairing the code, or implementing workarounds.

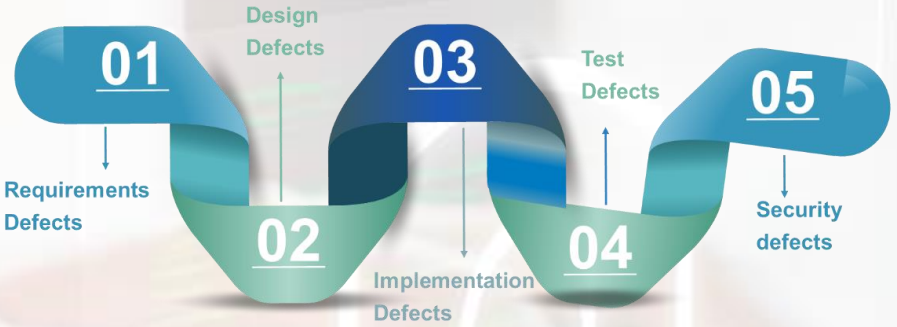
Monitoring and Reviewing

Defect management doesn't stop once defects have been fixed. It's important to continuously monitor and review systems to ensure that they remain secure and to identify any new defects that may arise.



Types of Defects

- **Requirements Defects:** These are defects that result from incomplete, ambiguous, or conflicting requirements. Examples include missing or unclear requirements, requirements that are contradictory or inconsistent, and requirements that are not testable.
- **Design Defects:** These are defects that result from an incorrect or incomplete design. Examples include design errors, design oversights, and design omissions.
- **Implementation Defects:** These are defects that result from incorrect or incomplete implementation of the design. Examples include coding errors, syntax errors, and logical errors.
- **Test Defects:** These are defects that result from incorrect or incomplete testing. Examples include missing or incorrect test cases, test cases that are not representative of real-world scenarios, and test cases that are not properly executed.
- **Security defects:** These are defects that result from malware, phishing, Denial of Service (DoS) attacks, SQL injection, and Cross-Site Scripting (XSS).



Defect Management Pre-requisites (Technology, Process, People)

A combination of technology, process, and people is required for effective defect management in software development.

- **Technology:** A good defect management system may have the right tools and technologies to track, prioritize, and resolve defects in systems and solutions. This might include a bug tracking tool, a version control system, and automated testing tools.
- **Process:** A well-defined and documented process for managing defects is crucial for ensuring that defects are identified, prioritized, and resolved in a timely and efficient manner. This process should include clear roles and responsibilities, a system for tracking and reporting defects, and a way to prioritize defects based on their impact and likelihood of occurrence.
- **People:** Defect management requires the involvement and cooperation of various stakeholders, including developers, testers, project managers, and customers. It is important to clearly understand each stakeholder's

roles and responsibilities and establish a culture of collaboration and continuous improvement.

The Benefits of Applying the Defect Management Capability

Incorporating this capability within entities will yield a multitude of benefits, such as:

- **Improved Security:** By identifying and fixing defects early on, Entities will reduce the risk of vulnerabilities being introduced in the systems. This can help to protect the product from potential security threats and reduce the risk of data breaches or other security incidents.
- **Enhanced Compliance:** A defect management process can help ensure that the product meets all necessary security and compliance standards. This can be particularly important for products that handle sensitive data or are used in regulated industries.
- **Better Risk Management:** By tracking and addressing defects in a systematic way, Entities will be able to manage the risks associated with the s. This can help to identify and mitigate potential security risks before they become a problem.
- **Enhanced Reputation:** By demonstrating a commitment to security and quality, Entities build trust with customers and improve the reputation of the entity. This can be particularly important in the context of cybersecurity, where the consequences of a security breach can be severe.
- **Reduced Costs:** Fixing defects early in the development process is usually cheaper than fixing them later. This is because it is easier to identify and fix defects when they are fresh in the developer's mind, rather than having to go back and try to understand the code after it has been written.
- **Increased Efficiency:** A defect management process helps to streamline the development process by identifying and fixing defects as they arise. This can help to reduce delays and increase efficiency in the development process.
- **Better End User Satisfaction:** ensuring that defects are identified and fixed quickly improves end-user satisfaction with the product.

2.8 Build Management Capability

Build management from a cyber security perspective involves ensuring that the security of a project or product is considered and integrated throughout the build process. This can include identifying and managing potential security risks, implementing appropriate security controls and safeguards, and verifying that the final product or project meets the required security standards.

Entities must thoroughly grasp cyber security principles and practices in order to effectively manage a project's build from a cyber security standpoint. This includes comprehension of common security risks and vulnerabilities and how to implement appropriate security controls and safeguards.

From a cyber security standpoint, effective build management entails several important activities, including the following:

- Identifying and assessing potential security risks that could impact the project and assessing the likelihood and potential impact of each risk.
- Implementing appropriate security controls and safeguards to mitigate those risks. This could include implementing encryption for sensitive data, implementing access controls to prevent unauthorized access, and implementing security monitoring to detect potential security breaches.
- Verifying the security of the final product or project to ensure that it meets the required security standards. This could include conducting security testing or vulnerability assessments or obtaining third-party certification to verify the security of the project.

Overall, managing a project's build from a cyber security perspective is an essential part of ensuring the security of the final product or project. By considering security throughout the construction process, Entities can minimize the risks of security breaches and ensure that the final product or project meets the required security standards based on the Software Bill of Materials and Software Component Analysis.

- A Software Bill of Materials (SBOM) is a list of all the components that comprise a piece of software, including their versions and source information. It is a detailed inventory of the software's components, often including open-source libraries, frameworks, and other third-party code. An SBOM can help entities track and manage their software's security and legal compliance, as well as ensure that all components are properly licensed and up-to-date. It can also help entities identify and address potential vulnerabilities in their software.
- Software Component Analysis is the process of identifying and analyzing the individual components that make up a piece of software. This includes identifying the source of each component, its version, any dependencies it has, and any potential vulnerabilities or security risks associated with it. By thoroughly analyzing the software's components, entities can better understand the security and legal implications of using the software and ensure that all components are properly licensed and up-to-date. This can help entities avoid potential legal issues and reduce the risk of security vulnerabilities.

Build Managing Prerequisites (Technology, Process, People)

The prerequisites for effective build management include the following:

- **Technology**: tools that can help to plan, coordinate, and track the progress of the construction process. This could include tools for project scheduling, risk management, and contract management, as well as tools for communication and collaboration.
- **Process**: Will establish processes and activities to identify, analyze, track, and manage potential cyber security issues during the build process.
- **People**: skilled and experienced individuals who can support the construction process. This could include architects, engineers, contractors, and other specialists, as well as project managers who can help to coordinate and manage the project.

The Benefits of Build Managing Capability Utilization

Incorporating this capability within entities will yield a multitude of benefits, such as:

- **Reduced Risk of Security Vulnerabilities**: By carefully tracking and managing the components that make up the software, entities can reduce the risk of security vulnerabilities and protect their software and users from potential threats.
- **Improved Compliance with Security Standards and Regulations**: By ensuring that all components are properly licensed and up-to-date, entities can improve their compliance with relevant security standards and regulations, such as the OWASP Top 10 or PCI DSS.
- **Increased Visibility and Control Over Software Security**: By maintaining a detailed inventory of the software's components, entities can gain greater visibility and control over the security of their software, and quickly identify and address any potential vulnerabilities.
- **Improved Incident Response Capabilities**: By knowing the components that make up their software, entities can more effectively respond to security incidents and quickly identify and fix any vulnerabilities that may have been exploited

2.9 Release Management Capability

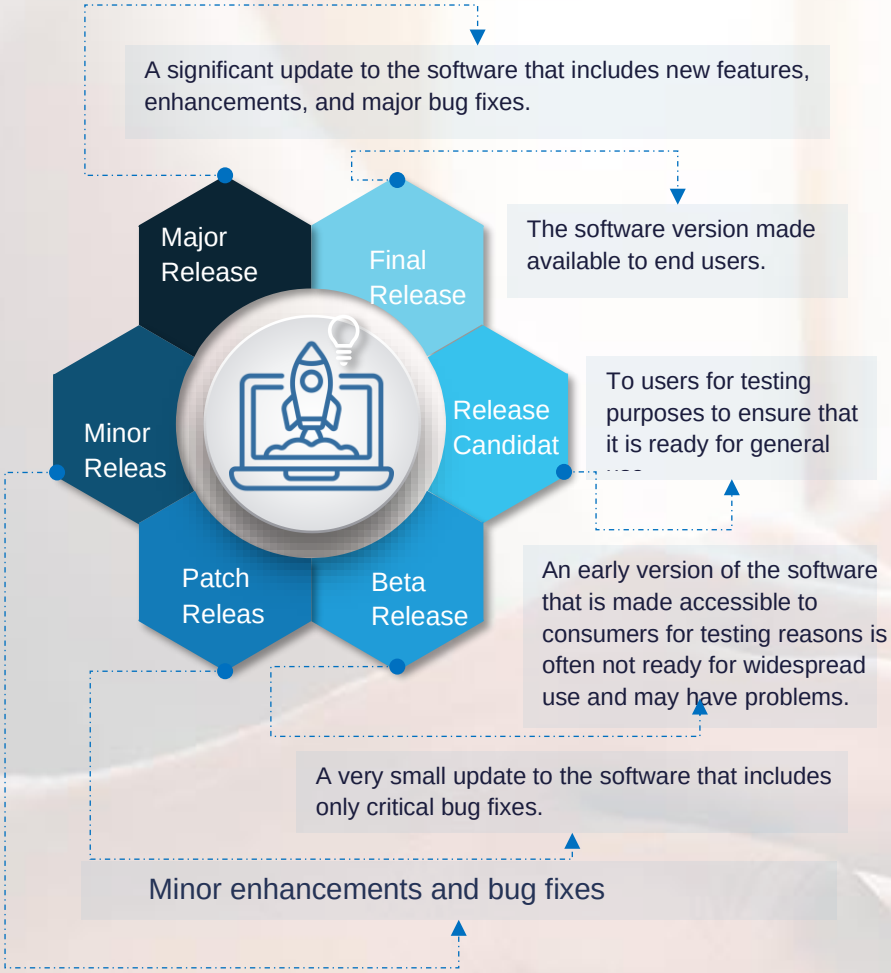
it's important to consider cybersecurity in the release management process to ensure the safe and secure deployment of software updates. This involves identifying and addressing potential security issues throughout the release process, emphasizing rigorous testing, strict access controls, and swift response mechanisms to maintain a secure environment during software releases.

Within the realm of Release Management, entities should prioritize upholding cybersecurity standards through training programs, comprehensive documentation, and regular checks to facilitate smooth and secure software releases.

Release Types

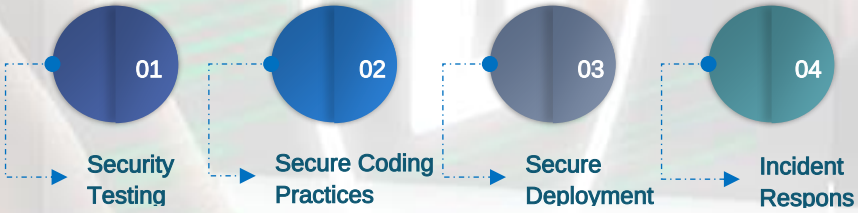
There are several types of releases, which differ based on their purpose and scope of impact, including:

- **Major Release:** A major release is typically a significant update to the software that includes new features, enhancements, and major bug fixes. Major releases are often accompanied by a change to the major version number of the software (e.g., from version 1.0 to 2.0).
- **Minor Release:** A minor release is a smaller update to the software that includes minor enhancements and bug fixes. Minor releases are typically accompanied by a change to the minor version number of the software (e.g., from version 1.1 to 1.2).
- **Patch Release:** A patch release is a very small update to the software that includes only critical bug fixes. Patch releases are typically accompanied by a change to the patch version number of the software (e.g., from version 1.1.1 to 1.1.2).
- **Beta Release:** A beta release is an early software version made available to users for testing purposes. Beta releases are typically not ready for general use and may contain bugs or other issues that need to be resolved before the final release.
- **Release Candidate:** A release candidate is a version of the software that is considered ready for release but is made available to users for testing purposes to ensure that it is ready for general use.
- **Final Release:** The final release is the software version made available to end users. This is the version of the software that is complete, stable, and ready for general use.



Effective release management within the field of cybersecurity requires various concepts related to cybersecurity, such as:

- **Security Testing:** As part of the release management process, it is important to conduct security testing to ensure that the software is secure and does not contain any vulnerabilities that could be exploited by hackers. This typically involves conducting various types of testing, such as penetration testing, vulnerability scanning, and code review, to identify and address any security issues.
- **Secure Coding Practices:** To ensure the security of a software release, it is important to follow secure coding practices during the development process. This includes using secure coding standards, avoiding common security pitfalls, and performing regular code reviews to ensure that the code is secure.
- **Secure Deployment:** To ensure the security of a software release, it is important to deploy the software in a secure manner. This may involve using secure communication channels, implementing access controls, and following best practices for securely deploying and managing software.
- **Incident Response:** In the event of a security incident, it is important to have a well-defined incident response plan in place to ensure that the situation is handled quickly and effectively. This typically involves establishing a team to respond to the incident, identifying the cause of the incident, and taking steps to prevent similar incidents from occurring in the future.



Overall, these concepts and principles are critical for ensuring the security of a software release and are essential for ensuring that the release is delivered promptly, efficiently, and effectively.

Release Management Pre-Requisites (Technology, Process, People)

- **Technology:** In order to manage the software development process effectively, it is important to have the right technology in place. This may

include tools for managing the release schedule, coordinating with different teams, and conducting cybersecurity testing.

- **Process:** In order to manage a software release effectively, it is important to have a well-defined process in place. This typically involves establishing clear roles and responsibilities, defining the release schedule, and establishing protocols for managing changes to the release.

- **People:** Effective release management requires the involvement of multiple teams, including development, security teams, quality assurance, and operations. It is important to have the right people in place, with the necessary skills and expertise, to ensure that the release is delivered on time and with the desired level of quality and functionality. This may include having a dedicated release manager to coordinate the efforts of the different teams.

The Benefits of Applying the Requirement Management Capability

Incorporating this capability within entities will yield a multitude of benefits, such as:

- **Improved Security:** Release management helps improve security by ensuring that software is tested and reviewed before it is released. This can help prevent the release of software with vulnerabilities or other security issues.

- **Better Control:** Release management provides better control over the software development and release process, which can help reduce the risk of unauthorized changes or modifications to the software.

- **Faster Response to Threats:** Release management allows entities to quickly respond to security threats by releasing patches and updates to fix vulnerabilities and other security issues.

- **Enhanced Compliance:** Release management can help entities comply with industry regulations and standards related to cyber security, such as the Payment Card Industry Data Security Standard (PCI DSS).

3 Security in Delivery

One of the most important methodologies in the service production life cycle is the service delivery security methodology. Security in delivery is a critical component of this methodology.

Security in Delivery refers to the measures taken to protect data and services during transformation and delivery. Such measures include secure encryption, tracking and monitoring systems, and personnel background checks on delivery. Security delivery aims to ensure that services/data are delivered to the intended recipient safely and securely without being lost, stolen, or tampered with during transit.

Security in delivery capability has several key elements, including:

ENCRYPTION

Encryption is the process of converting plain text into a coded format that only authorized parties with the appropriate decryption key can read. This helps to prevent unauthorized parties from intercepting and reading.

AUTHENTICATION

Authentication is the process of verifying the identity of the data sender and receiver. This helps to prevent unauthorized access to sensitive information and ensures that data can only be received and transmitted by authorized parties.

ACCESS CONTROL

Access control is the process of managing access to data and resources based on predefined security policies. This helps to prevent unauthorized access to sensitive information and ensures that only authorized parties can access and use data.

NETWORK SECURITY

Network security entails safeguarding networks and systems against attacks and unauthorized access. Examples include firewalls, intrusion detection and prevention systems, and other security technologies.

Overall, security in delivery is a critical aspect of cybersecurity that helps to protect data and information while it is being transmitted or delivered over a network. By implementing strong encryption, authentication, access control, and network security measures, entities can help to ensure the confidentiality, integrity, availability, and safety of sensitive information or services

A Comprehensive Overview

The following exposition provides a comprehensive overview of this main capability and its sub-capabilities among its counterparts to provide a detailed analysis of the capability and its components. By minding this capability and its sub-capabilities, entities can gain insights into how they interact and utilize it to achieve the desired outcomes according to their field and business requirements. This overview is intended to serve as a valuable reference for understanding this critical capability.

3.1 Resource Management

Resource Management capability in cybersecurity refers to the strategic allocation, optimization, and protection of various resources within an entity to effectively manage and mitigate cyber threats. These resources include hardware, software, network infrastructure, personnel, budget, and information assets. The primary objective of resource management in cybersecurity is to ensure the availability, confidentiality, and integrity of critical systems and data while efficiently utilizing limited resources.

Below is a comprehensive overview of the fundamental elements and constituents comprising the Resource Management capability in the field of cybersecurity:

- **Resource Inventory:** An essential step in resource management is creating an inventory of all the assets involved in cybersecurity. This includes hardware devices (e.g., servers, routers, firewalls), software applications, databases, network components, and other critical systems. The inventory helps in identifying and categorizing resources based on their importance and vulnerability.
- **Risk Assessment:** Resource management involves assessing the risks associated with each resource. This includes identifying potential vulnerabilities, threats, and the potential impact of a cyberattack on each resource. Risk assessment helps prioritize resource allocation and protection efforts based on the level of risk and potential consequences.
- **Resource Allocation:** Once the risks are assessed, resource allocation decisions are made to ensure optimal utilization of available resources. This includes determining the allocation of budget, personnel, and technology solutions to different areas of cybersecurity, such as network security, endpoint protection, data encryption, access controls, and incident response.
- **Resource Optimization:** Resource optimization focuses on maximizing the efficiency and effectiveness of cybersecurity resources. This involves implementing best practices, automation, and intelligent resource allocation techniques to minimize resource wastage, reduce manual effort, and enhance overall security posture. It may also involve consolidating and rationalizing resources to eliminate duplication and streamline operations.
- **Budget Management:** Managing the cybersecurity budget is a crucial aspect of resource management. It involves allocating funds for various security initiatives, such as purchasing and maintaining security tools, conducting audits, training personnel, and implementing security measures. Effective budget management ensures that adequate resources are available to address evolving cyber threats and maintain a robust security infrastructure.
- **Personnel Management:** Cybersecurity resource management also includes managing the human resources involved in cybersecurity, such as security analysts, administrators, incident responders, and other staff. This involves recruiting, training, and retaining skilled professionals, as well as establishing clear roles and responsibilities, conducting performance

evaluations, and providing ongoing professional development opportunities.

Resource Management Prerequisites (Technology, Process, People)

- **Technology:**
  Management Systems: These systems aid in identifying and maintaining an inventory of all cybersecurity resources, including human resources, hardware, software, and network components.

  Automation and Orchestration Tools (optional): These technologies automate routine tasks, streamline resource allocation processes, and enhance overall efficiency.

- **Processes**
  Resource Allocation Policies: Policies that guide the allocation of cybersecurity resources based on risk analysis, business needs, and regulatory requirements.

  Regular Auditing and Monitoring: Processes to continuously monitor resource usage, conduct audits, and track compliance with established resource management policies.

- **People**
  Training and Awareness: People involved in resource management are responsible for training and creating awareness among employees about the importance of cybersecurity resources. They conduct training programs to educate employees on security best practices, resource utilization guidelines, and potential risks. This helps in ensuring that employees understand their role in protecting resources and adhere to established security policies and procedures.

By fulfilling these technology, process, and people prerequisites, entities can establish a strong cybersecurity Resource Management capability, enabling effective allocation, optimization, and protection of resources to mitigate cyber risks and threats.

The Benefits of Applying the Resource Management Capability

Incorporating this capability within entities will yield a multitude of benefits, such as:

- **Efficient Resource Allocation:** Resource Management enables entities to allocate cybersecurity resources efficiently based on risk assessments and entityal priorities, maximizing their effectiveness while minimizing waste.

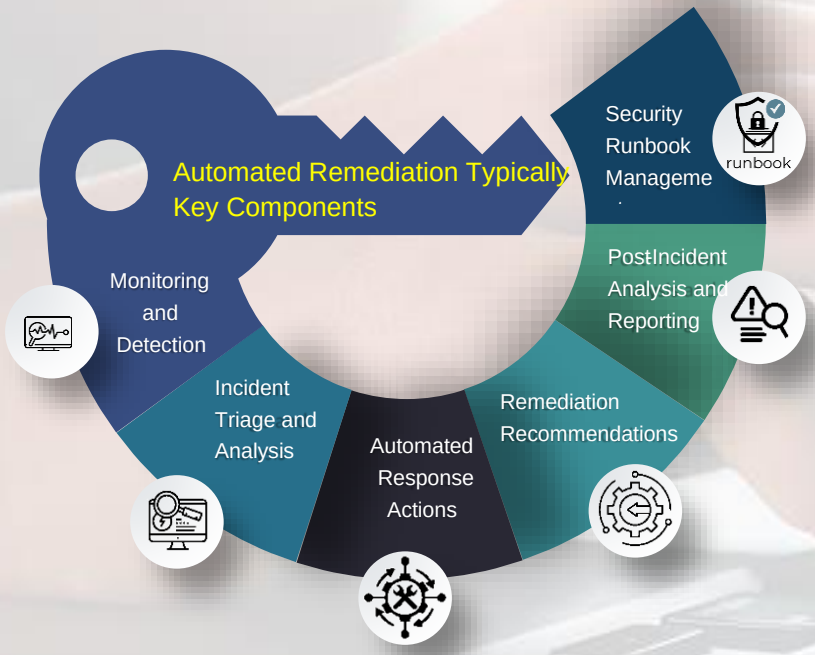
- **Cost Optimization:** By strategically allocating resources, entities can optimize costs associated with cybersecurity, ensuring budget allocation aligns with critical security needs.

- **Enhanced Security Posture**: Resource Management contributes to an improved security posture by strengthening defense mechanisms, protecting critical assets, and reducing the risk of successful cyberattacks.
- **Effective Incident Response**: Resource Management supports effective incident response capabilities by identifying and allocating necessary resources, ensuring swift and efficient response to cyber incidents.
- **Compliance and Regulatory Adherence**: Resource Management helps entities meet compliance requirements and adhere to regulatory standards, enhancing trust and demonstrating a commitment to security.
- **Optimal Staffing and Skill Utilization**: Resource Management ensures optimal utilization of cybersecurity personnel by aligning resource needs with staff expertise, maximizing their efficiency in areas where their skills are most valuable.
- **Continual Improvement**: Resource Management facilitates continual improvement in cybersecurity practices by monitoring resource usage, evaluating effectiveness, and adapting resource allocation strategies to address emerging threats and challenges.

3.2 Automated Remediation

Automated remediation is considered the process of automatically finding and fixing security problems, vulnerabilities, or events within an entity's system or network infrastructure. This groundbreaking method combines the power of artificial intelligence (AI) and machine learning (ML) with cutting-edge security solutions for quick detection, analysis, and threat mitigation. Finding, examining, and fixing security problems and incidents within an entity's network or system infrastructure. By quickly recognizing and eliminating security threats in close to real-time, this proactive strategy seeks to reduce the effect of security concerns.

Automated remediation typically involves several key components, including:



- **Monitoring and Detection:** Uses artificial intelligence and machine learning algorithms to analyze, monitor, and detect trends, behaviors, and anomalies that may indicate vulnerabilities or security vulnerabilities
- **Incident Triage and Analysis:** Once an incident is detected, the automatic remediation system assesses its severity and impact to determine the appropriate response actions.
- **Automated Response Actions:** Using specified Runbooks or rules, the system can carry out automated reaction actions.
- **Post-Incident Analysis and Reporting:** Following the resolution of an incident, the automatic remediation system does post-incident analysis to find any underlying issues, flaws, or vulnerabilities that may have contributed to the occurrence.
- **Remediation Recommendations:** The system can suggest to security analysts or administrators when automated response activities might not be appropriate or need human validation.
- **Security Runbook Management:** Security runbook management is a systematic approach to organizing, documenting, and executing predefined procedures and processes for addressing security incidents and events within an entity. It provides a standardized framework that guides security teams in effectively responding to and mitigating security threats.

  The main goal of security runbook management is to streamline the workflow of incident response, increase consistency, and improve the efficiency of security operations. It involves developing comprehensive runbooks that provide detailed instructions, guidelines, and response procedures for different security incidents, such as malware infections, data breaches, system compromises, or network intrusions.

  When combined with automated remediation, security runbook management enhances the efficiency, speed, and consistency of incident response and mitigation efforts. This method brings together the advantages of automated remediation technology and the structured and documented procedures of security runbooks, creating a powerful framework for proactive incident management.

Automated Remediation Pre-requisites (Technology, Process, People)

To ensure optimal utilization of this capability, it is imperative to fulfill the following prerequisites:

Technology:

Security Information and Event Management (SIEM) System: The SIEM system forms the foundation for automated remediation. It collects and correlates security event data from various sources, providing real-time visibility into potential security incidents.

Threat Intelligence: Access to up-to-date threat intelligence feeds and databases is crucial. It enables the automated remediation system to accurately analyze and detect emerging threats, facilitating proactive incident response.

Security Orchestration, Automation, and Response Platform: (SOAR) A platform integrates with the SIEM system and other security tools to automate response actions and orchestrate incident management processes. It provides the necessary automation and workflow capabilities for executing remediation actions.

Processes:

Incident Response Framework: Establishing a well-defined incident response framework is crucial. It outlines the processes, roles, and responsibilities of the incident response team, including incident categorization, triage, investigation, and remediation.

Runbook Development: Developing comprehensive runbooks is a critical process for automated remediation. These runbooks document step-by-step procedures for addressing various security incidents. They outline response actions, recommended tools, and the sequence of tasks to be performed during incident remediation.

People:

Security Experts: Qualified security professionals, including incident response analysts, threat intelligence experts, and system administrators, are essential for the successful implementation and operation of automated remediation.

Collaboration and Communication: Effective collaboration and communication between security teams, IT teams, and other stakeholders is critical to clearly defining and communicating incident response processes and roles to ensure a coordinated and cohesive approach to incident management.

Training and Awareness: Providing adequate training and awareness programs to security teams on using automated remediation technology, runbooks, and incident response processes are important. This ensures they are well-equipped to leverage the automated remediation capabilities and maximize the effectiveness of incident response efforts.

The Benefits of Applying the Automated Remediation Capability

Incorporating this capability within entities will yield a multitude of benefits, such as:

- **Rapid Incident Response:** Automated remediation can detect and respond to security incidents in real-time or near-real-time. This swift response helps mitigate the impact of cyber threats, reducing potential damage and data loss.
- **Continuous Compliance Logging:** Automated remediation tools maintain real-time compliance by promptly addressing any deviations from established security standards. This ensures ongoing adherence to regulatory requirements and creates a comprehensive audit trail. It reduces compliance risk, offers immediate correction, and bolsters transparency during audits, enhancing a business's security posture.
- **Minimize Human Error and Resource Optimization:** Automation reduces human error in cybersecurity by precisely handling routine tasks. Security teams can redirect their efforts from repetitive activities to strategic tasks like threat hunting and proactive risk mitigation. This leads to cost efficiencies, faster incident response, and, ultimately, a stronger cybersecurity defense.
- **Mitigation of Known Vulnerabilities:** Automated systems can identify and patch known vulnerabilities in software and systems as soon as patches become available, reducing the window of opportunity for attackers to exploit these weaknesses.
- **Scalability:** Automated remediation scales effectively with the size and complexity of the IT environment. It can handle a growing number of devices, systems, and endpoints without requiring a proportional increase in human resources.
- **Reduced Downtime:** Automated responses to security incidents can help minimize system downtime and disruptions, ensuring business continuity even in the face of cyberattacks.
- **Data Protection:** Automated remediation can help safeguard sensitive data by swiftly responding to data breaches and unauthorized access attempts. This is critical for protecting customer data and maintaining trust.

3.3 Request Management

Requests management is a key part of the cybersecurity plan. This means creating clear and security-focused rules that follow industry standards and rules. Doing careful risk assessments is really important. It involves putting requests in order based on how much they might affect security and making sure to respond quickly and effectively to those that could turn into security problems.

Connecting request management with the plan for handling security incidents is crucial. They need to fit with the overall cybersecurity plan and help find possible problems. Having strong processes to check who can access sensitive information is also necessary to avoid risks from requests that shouldn't be allowed.

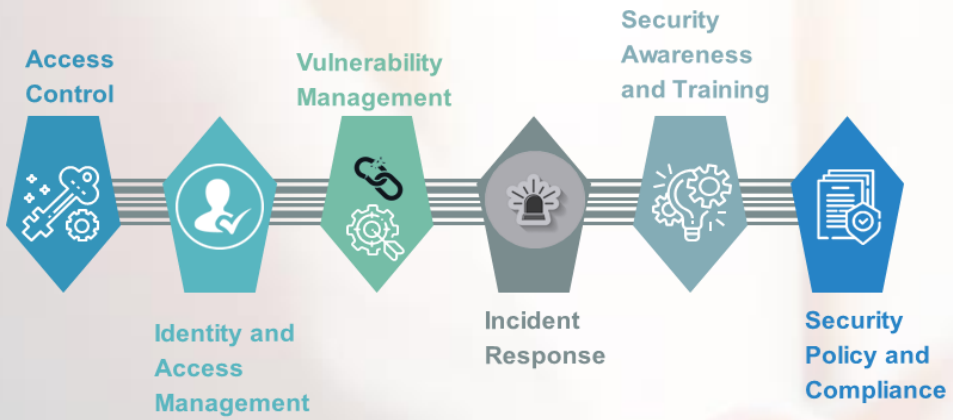
In order to effectively manage requests, it is important to establish clear policies and procedures, prioritize based on factors such as importance, impact, and urgency, and utilize tools for tracking. Monitoring metrics such as response time, resolution time, and customer satisfaction are recommended to gauge the process's effectiveness. Additionally, possessing strong communication and customer service skills is essential.

Types of Requests

Various types of requests can be handled through request management processes, such as:

- **Service Requests**: These are requests for a specific service or product, such as installing new software or providing technical support.
- **Information Requests**: These are requests for information or data, such as reports, documents, or statistics.
- **Change Requests**: These are requests for changes to be made to existing services or products, such as modifications to software or updates to policies and procedures.
- **Problem-Solving Requests**: These are requests related to issues or problems that need to be resolved, such as technical problems or customer complaints.
- **Project Requests**: These are requests related to specific projects or initiatives, such as requests for resources or funding.
- **Approval Requests**: These are requests for approval or permission to move forward with a specific action or decision.
- **Feedback Requests**: These are requests for feedback or input on a particular topic or issue.
- **Complaint Requests**: These are requests related to complaints or dissatisfaction with a service or product.

Effective request management within the field of cybersecurity requires various concepts related to cybersecurity, such as:



- **Access Control:** Ensuring that only authorized users have access to specific resources or information. This may involve managing requests for access to systems or data, and enforcing access control policies.
- **Identity and Access Management:** Managing the identity and access of users to systems and resources. This may involve managing requests for new user accounts or access to specific systems or data.
- **Vulnerability Management:** Identifying and mitigating vulnerabilities in systems and networks. This may involve managing requests for vulnerability assessments or for the implementation of security patches or updates.
- **Incident Response:** Responding to and managing cyber incidents or threats. This may involve managing requests for incident response support or for the investigation of potential security breaches.
- **Security Awareness and Training:** Providing training and awareness to users on cybersecurity best practices. This may involve managing requests for security training or awareness materials.
- **Security Policy and Compliance:** Ensuring that security policies and procedures are in place and followed and that the entity is compliant with relevant laws and regulations. This may involve managing requests for policy updates or for compliance assessments.

Request Management Pre-Requisites (Technology, Process, People)

- **Technology:** Request management system or software, Project management tool, Customer relationship management (CRM) system, Help desk system, Firewall and intrusion detection systems, Security information and event management (SIEM) tools, and Data loss prevention (DLP) systems
- **Process:** Receiving requests, Triaging requests, Prioritizing requests, Tracking requests, Escalating requests, Communicating with stakeholders, Identifying and verifying the legitimacy of cybersecurity-related requests, Determining the appropriate response to cybersecurity-related requests, Documenting and tracking cybersecurity-related requests,
- **People:** Dedicated professionals with strong communication, problem-solving, and entity skills Team of cybersecurity professionals with expertise in cybersecurity, data protection, and risk management

Other factors that may be important for effective request management, including cybersecurity, include clear roles and responsibilities, policies and procedures, employee training and awareness programs, and adequate resources and budget.

The Benefits of Applying the Request Management Capability

Incorporating this capability within entities will yield a multitude of benefits, such as:

- **Improved Security** Properly managing and controlling request management can help reduce the risk of delayed response to vulnerabilities and issues being introduced into or discovered in the entity's systems.
- **Enhanced Control** Request management provides a structured and controlled process for deploying software, hardware, and updates, which can help reduce the risk of security incidents or breaches.
- **Improved Compliance** Request management can help entities stay compliant with regulatory requirements and industry best practices by ensuring that changes and updates are deployed in a controlled and documented manner.
- **Improved Communication** Effective communication with stakeholders, including requestors and those responsible for fulfilling requests
- **Continuous Improvement and Visibility** continuous improvement can help entities identify and address any weaknesses or inefficiencies in their request management process.

3.4 Change Management

Change Management is a critical component of an entity's cybersecurity strategy, and the cybersecurity process should guarantee that every change made in the entity is secure and ensure the entity's safety as well.

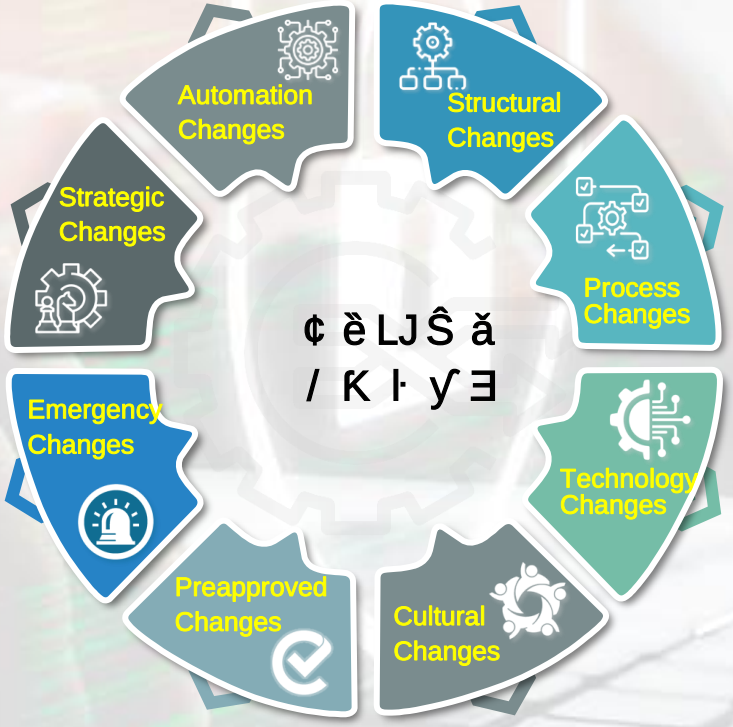
The changes may bring about unanticipated problems, so entities need to be on the lookout for these and be prepared to respond quickly and decisively if there are any security concerns. Entities must guarantee the security of their systems by closely monitoring the processes and outcomes of change. More specifically, it is critical to concentrate on those that might jeopardize security.

Ensuring proper cybersecurity measures during the initial stages of any change process is paramount. It is crucial to align all regulations with optimal security protocols to prevent any potential security breaches. This proactive approach will not only mitigate risks but also safeguard against any potential security threats. Therefore, it is imperative to prioritize cybersecurity and take necessary steps to promote a secure environment right from the outset.

Types of Change

To broaden perceptions of different types of change, we include (but are not limited to) the following as examples of changes that may occur or be introduced in entities:

- **Automation Changes**: processes built into a tool that automatically promotes software changes from one environment to another without the need for additional human intervention.
- **Structural Changes**: Changes to the entityal structure or design of an entity.
- **Strategic Changes**: Changes to an entity's overall direction or strategy.
- **Emergency Changes**: Changes to correct immediate issues that cause service disruption.
- **Preapproved Changes**: Changes that frequently occur, low-risk changes that a CAB or other appropriate approver has authorized for implementation.
- **Cultural Changes**: Changes to the values, beliefs, or behaviors of individuals within an entity.
- **Technology Changes**: Changes to the technologies used by an entity.
- **Process Changes**: Changes to the processes or procedures used by an entity.



Effective change management within the field of cybersecurity requires various concepts related to cybersecurity, such as:

- **Risk Measurement and Management:** This involves identifying, measuring, and managing the risks associated with cybersecurity-related systems or process changes. This may include conducting risk measurement, implementing controls to mitigate risks, and monitoring the effectiveness of these controls.
- **Stakeholder Engagement and Communication:** Engaging with stakeholders affected by cybersecurity-related systems or process changes. This may include educating stakeholders about the changes and potential impacts and seeking input and feedback to address their needs and concerns.
- **Training and Support:** This involves providing training and support to individuals affected by cybersecurity-related systems or process changes. This may include training on new technologies or processes and offering support to help individuals adapt to the changes.
- **Change Impact Measurement:** This involves measuring the potential impacts of changes to cybersecurity-related systems or processes on the entity and its stakeholders. This may include identifying potential risks or challenges, as well as identifying potential benefits or opportunities.
- **Change Management Processes and Tools:** This involves implementing change management processes and tools to effectively manage changes to cybersecurity-related systems or processes. This may include using change management frameworks, tools, or methods to plan, implement, and monitor the changes.

Change Management Prerequisites (Technology, Process, People)

To ensure optimal utilization of this capability, it is imperative to fulfill the following prerequisites:

- **Technology:** Effective change management requires entities to have suitable technology tools and systems. This includes utilizing change management software, automated tracking and reporting tools, and robust security monitoring systems.
- **Process:** Well-defined and documented change management processes are essential. This involves establishing clear roles and responsibilities, defining change request procedures, conducting risk assessments, and maintaining open communication channels throughout the change management lifecycle.
- **People:** Skilled and knowledgeable personnel are critical for successful change management. Entities should have a dedicated cybersecurity team that comprehends the potential risks associated with changes and possesses the expertise to implement appropriate security measures. Regular training and awareness programs should be conducted to ensure employees understand their responsibilities and are up-to-date with best practices.

The Benefits of Applying the Change Management Capability

Incorporating this capability within entities will yield a multitude of benefits, such as:

- **Reduced Risk Of Security Breaches:** Entities can reduce the likelihood of security breaches by identifying and addressing potential vulnerabilities or risks as part of the change management process.
- **Improved Compliance:** By implementing changes in a controlled and orderly manner, entities can ensure that they comply with relevant laws and regulations, including those related to cyber security.
- **Enhanced Reputation:** By effectively managing and mitigating potential security risks, entities can protect their reputation and avoid the negative consequences of security breaches.
- **Improved Efficiency and Productivity:** By identifying and addressing areas for improvement, change management can help entities to streamline their processes and work more efficiently. This can lead to increased productivity and cost savings.
- **Enhanced Customer Satisfaction:** Entities can enhance customer satisfaction and loyalty by making changes that improve the quality and reliability of products or services.
- **Greater Adaptability and Competitiveness:** Change management can help entities respond more quickly and effectively to changing market conditions and customer needs, increasing their competitiveness.
- **Improved Morale and Engagement:** By involving employees in the change process and seeking their input and feedback, entities can improve morale and engagement, leading to better performance and higher retention.

3.5 Identity & Access Management

Identity and Access Management (IAM) is a crucial process and technology used to manage users' digital identities and the resources they have access to. It involves managing the entire lifecycle of user identities, including account creation, maintenance, and retirement.

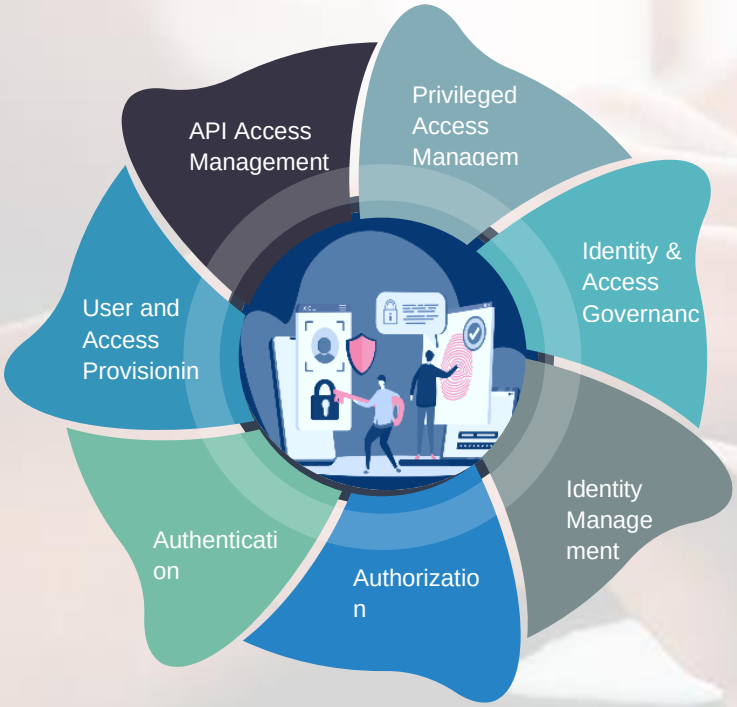
Identity and Access Management plays a vital role in cybersecurity as it involves the processes and technologies for managing and controlling access to an entity's systems and data. It ensures that only authorized individuals or entities can access their systems and data, preventing unauthorized access and potential security breaches.

Identity and Access Management systems are critical in helping entities secure their networks and resources, ensuring that only authorized users have access to sensitive information.

- **Identity & Access Governance:** Identity & Access Governance (IAG), is a broad and strategic concept. It encompasses the technical aspects and the policies, procedures, and governance structures related to identity and access control. IAG focuses on ensuring that identities and their access rights align with business objectives, compliance requirements, and risk management. It involves defining and enforcing policies, reviewing and certifying user access, and monitoring for compliance.
- **Identity Management:** Identity Management (IdM), primarily focuses on the technical aspects of creating, managing, and controlling digital identities and their associated access rights. It involves tasks such as user provisioning, authentication, authorization, and de-provisioning. Identity Management is concerned with ensuring that the right individuals have the appropriate access to systems, applications, and data.
- **Authorization Management:** Authorization Management refers to the process of granting or denying access to specific digital resources or systems based on the rights and permissions of individual users. This is typically done through the use of an authorization system, which is a component of an identity and access management (IAM) system. An authorization system allows an entity to define each user's specific rights and permissions and enforce those permissions when a user attempts to access a particular resource.
- **Authentication Management:** Authentication Management refers to verifying the identity of users attempting to access an entity's digital resources or systems. This typically involves using authentication technologies, such as passwords, biometric scanners, or security tokens, to verify a user's identity before allowing access to a particular resource.
- **API Access Management:** API Access Management in cybersecurity refers to the process of controlling and securing access to an entity's application programming interfaces (APIs). APIs are a common method for allowing different applications or services to communicate with each other, and they can provide access to sensitive data or functionality within an entity's systems. As a result, it is important to carefully manage and control access to APIs in order to prevent unauthorized access or misuse.
- **User and Access Provisioning:** User and Access Provisioning in cybersecurity refers to the process of creating and managing user accounts and access to an entity's digital resources and systems. This typically involves implementing technologies such as identity and access management (IAM)

systems, which are used to create and manage user accounts and to authenticate and authorize users to access specific resources.

- **Privileged Access Management:** Privileged Access Management (PAM) is the process of controlling and securing access to an entity's sensitive systems and data by privileged users. Privileged users are individuals who have special access rights or permissions that allow them to perform sensitive or critical tasks within an entity's systems. These tasks might include managing user accounts, configuring security settings, or accessing sensitive data.



Identity & Access Management Capability Prerequisites (Technology, Process, People)

There are several prerequisites for implementing an effective identity and access management (IAM) system, including the following:

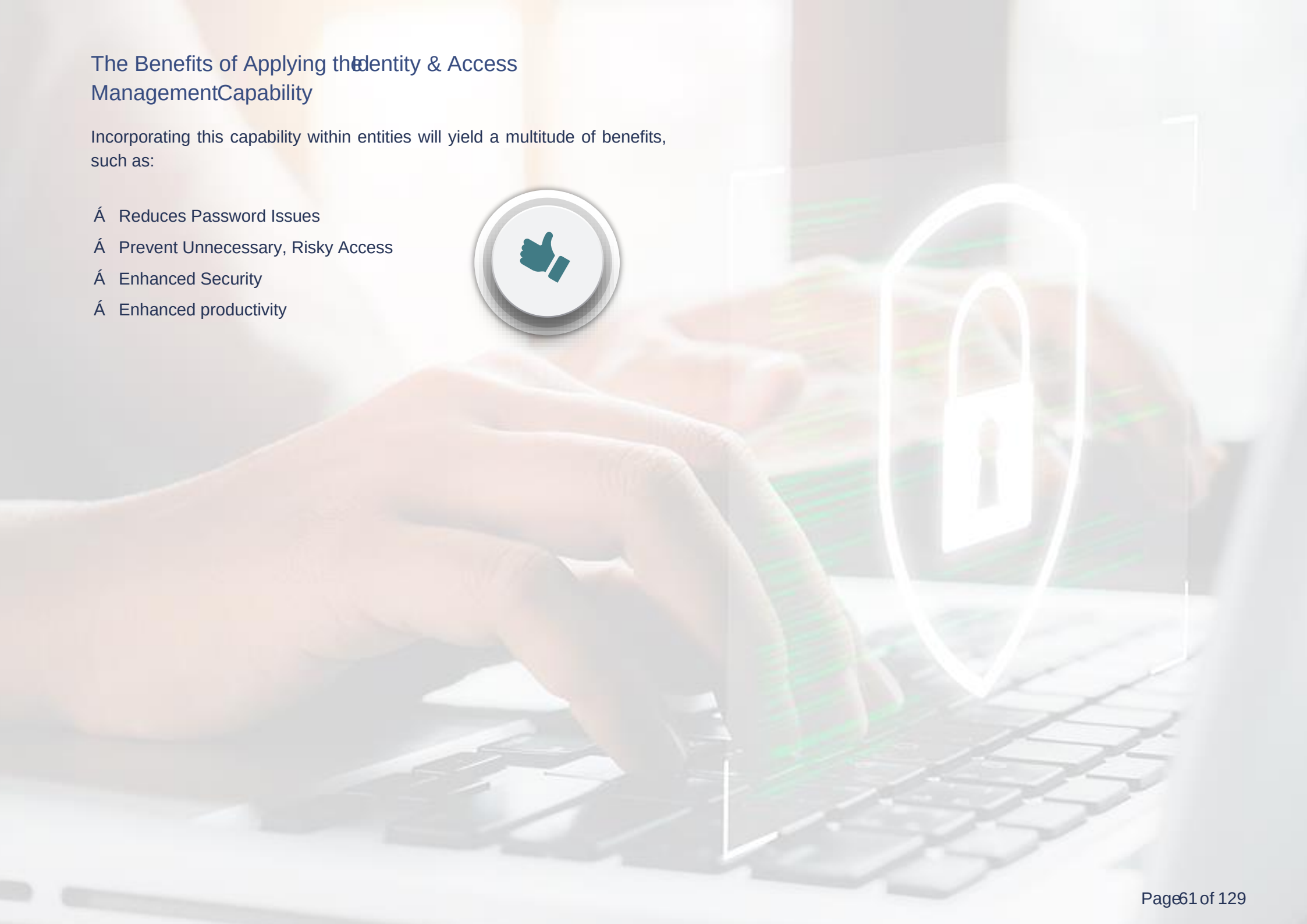
- **Technology:** Identity and Access Management systems typically require the use of specialized software and hardware to manage and control access to digital resources and systems. This might include authentication servers, access control systems, and other types of security infrastructure.
- **Process:** Identity and Access Management systems require well-defined processes and procedures for managing and controlling user access to resources. This might include policies for creating and managing user accounts, authenticating users, authorizing access to specific resources, and monitoring and managing user access.
- **People:** Identity and Access Management systems require the involvement of people at various levels within an entity, including system administrators, security personnel, and other individuals who are responsible for managing and controlling access to resources. These individuals need to be trained and empowered to implement and enforce IAM policies and procedures.

Overall, the successful implementation of an Identity and Access Management system requires a combination of the right technology, processes, and people to ensure that user access to digital resources and systems is managed and controlled effectively.

The Benefits of Applying the Identity & Access Management Capability

Incorporating this capability within entities will yield a multitude of benefits, such as:

- Reduces Password Issues
- Prevent Unnecessary, Risky Access
- Enhanced Security
- Enhanced productivity



3.6 Deployment/Provisioning

In Cybersecurity, deployment/provisioning refers to installing and configuring security systems, software, and hardware on a network or device, including installing antivirus software, firewalls, intrusion prevention systems, and other security measures to protect against cyber threats. It also entails implementing access controls, user permissions, and policies to ensure that only authorized users can access confidential data and resources

The deployment/provisioning process is critical in maintaining a mature Cybersecurity environment, as it ensures that all necessary security measures are in place and deployed against potential threats.

When deploying cybersecurity measures, many factors must be considered, including:

- The entity's size and complexity.
- The types of data and systems that are safeguarded.
- The level of risk that the entity is willing to take.
- A well-defined security plan is in place and is reviewed and updated regularly.
- Regularly update the used security measures to ensure their effectiveness in protecting against evolving threats

1.3.6.1.1 Patch Management

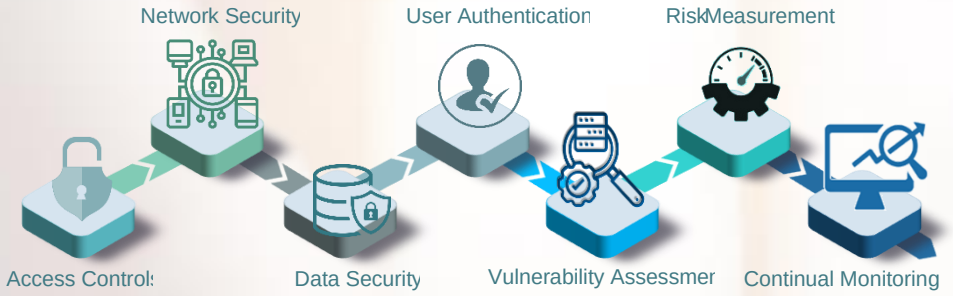
Patch management is the process of identifying, testing, and implementing software updates or patches to fix vulnerabilities and improve the security of a system. It is an essential aspect of cybersecurity because it helps protect against potential attacks and exploits that could compromise the system.
There are several steps involved in patch management, which are:

- **Identify Vulnerabilities** This involves regularly scanning the system to identify any vulnerabilities that may exist. This can be done using tools like vulnerability scanners or by manually reviewing system logs and security reports.
- **Test Patches** Once vulnerabilities are identified, patches or updates are created to fix them. It is important to test these patches thoroughly to ensure that they do not introduce any new vulnerabilities or cause other issues.
- **Implement Patches** After testing, patches are implemented on the system. This may involve scheduling downtime or rolling out the patch in stages to minimize disruption.
- **Monitor Systems** It is important to monitor systems after patches have been implemented to ensure that they are working correctly and that the vulnerabilities have been successfully fixed.

Overall, effective patch management is crucial to maintaining the mature security environment of a system and protecting against potential attacks.

1.3.6.1.2 Secure Deployment

Secure deployment refers to the process of deploying software or hardware in a secure manner. This includes ensuring that all necessary security measures are in place and that any vulnerabilities are identified and addressed before deployment.
The following are some key deployment security considerations:



- **Access Controls:** Ensure that only authorized personnel have access to the software or hardware being deployed.
- **Network Security:** Ensure that the network is secure and that all necessary firewalls and security protocols are in place.
- **Data Security:** Ensure that all data is encrypted and that only authorized users have access to it.
- **User Authentication:** Implement strong user authentication measures to prevent unauthorized access.
- **Vulnerability Assessment:** Conduct a thorough vulnerability assessment to identify any potential weaknesses and address them before deployment.
- **Risk Measurement:** Identify and assess any potential risks associated with the deployment and implement measures to mitigate these risks.
- **Continual Monitoring:** Monitor the system regularly to ensure that all security measures are in place and functioning properly.

Deployment/Provisioning Prerequisites (People, Process, Technology)

A combination of technology, process, and people are required for an effective Deployment/Provisioning process.

- **People:** Trained and skilled cybersecurity personnel to design and implement secure systems and networks; security analysts to monitor and detect potential threats; Incident response team to handle and contain security breaches.
- **Process:** Well-defined security policies and procedures to ensure compliance and mitigate risks; regular security assessments and audits to identify and address vulnerabilities; clear communication and collaboration among all stakeholders involved in deployment and provisioning.
- **Technology:** Automated Tools might be used to enhance the process of identifying and analyzing cybersecurity issues while deploying services, solutions, software, and hardware.

The Benefits of Applying the Deployment/Provisioning Capability

Incorporating this capability within entities will yield a multitude of benefits, such as:

- Ensure the security of services, solutions, systems, and devices.
- Ensure that users have the necessary access and permissions to carry out their duties.
- Prevent unauthorized access and data breaches
- Ensure the protection of the entity's assets and services
- Reduces the likelihood of errors or mistakes during setup and configuration, leading to fewer issues and downtime.

3.7 Secrets Management

Secrets Management in cyber security refers to the process of securely storing, protecting and managing sensitive information such as passwords, API keys, and encryption keys. This is important because these secrets can be used to access systems, data, and networks, and if they are compromised, it can lead to serious consequences such as data breaches and cyber attacks.

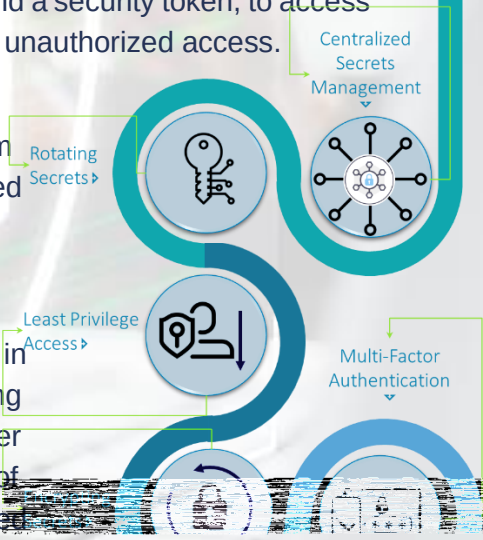
Secrets management is a cybersecurity best practice for digital businesses, allows entities to consistently enforce security policies for non-human identities.

Secrets management assures that resources across tool stacks, platforms, and cloud environments can only be accessed by authenticated and authorized entities. Many of these approaches and techniques are also used to protect privileged access by human users. The following steps are typically included in a secrets management initiative

- Authenticate all access requests that use non-human credentials.
- Enforce the principle of least privilege.
- Enforce role-based access control and regularly rotate secrets and credentials.
- Automate management of secrets and apply consistent access policies.
- Track all access and maintain a comprehensive audit.
- Remove secrets from code, configuration files, and other unprotected areas.

The secrets management capability includes several key features and functions that help to ensure the secure handling of sensitive data. These include:

- **Centralized Secrets Management:** This involves storing secrets in a central repository, such as a password manager or secrets management tool, that is accessed by authorized users only. This helps to prevent secrets from being stored in plain text or shared unnecessarily.
- **Least Privilege Access:** This involves granting access to secrets only to those who need it for their job duties and responsibilities. This helps to reduce the risk of secrets being accessed by unauthorized individuals.
- **Rotating Secrets:** This involves regularly changing secrets, such as passwords or API keys, to prevent them from being compromised.
- **Multi-Factor Authentication:** This involves using multiple methods of authentication, such as a password and a security token, to access secrets. This helps to reduce the risk of unauthorized access.
- **Encrypting secrets:** This involves encrypting secrets to protect them from being accessed by unauthorized individuals.



Overall, effective secrets management in cyber security is essential to protecting sensitive information and preventing cyber attacks. It involves a combination of strategies to ensure that secrets are stored securely, accessed only by authorized individuals, and regularly rotated to reduce the risk of compromise.