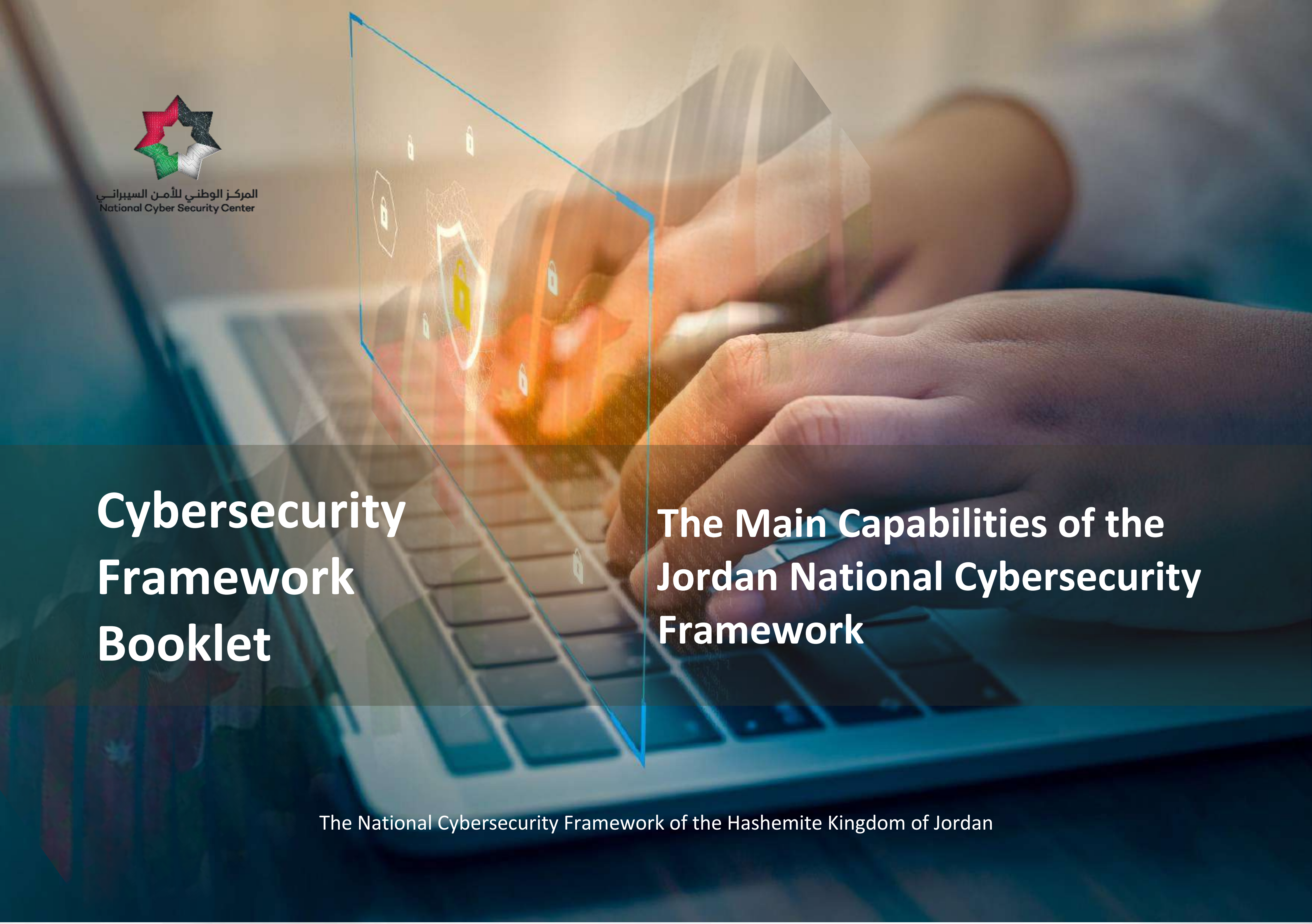


المركز الوطني للأمن السيبراني
National Cyber Security Center

# Cybersecurity Framework Booklet

## The Main Capabilities of the Jordan National Cybersecurity Framework

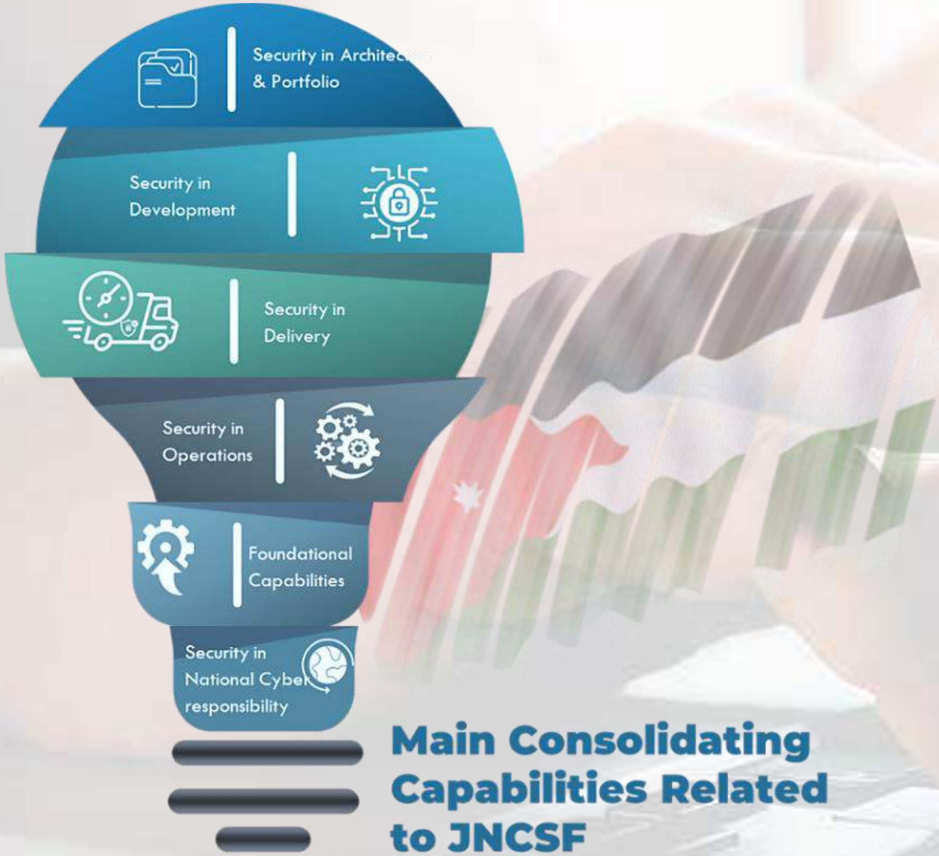
The National Cybersecurity Framework of the Hashemite Kingdom of Jordan

# Table of Contents

## Jordan National Cybersecurity Framework Capabilities

The Jordan National Cybersecurity Framework requires all entities, private and government, to build and develop entityal 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:



Main Consolidating Capabilities Related to JNCSF

- **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 services 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.

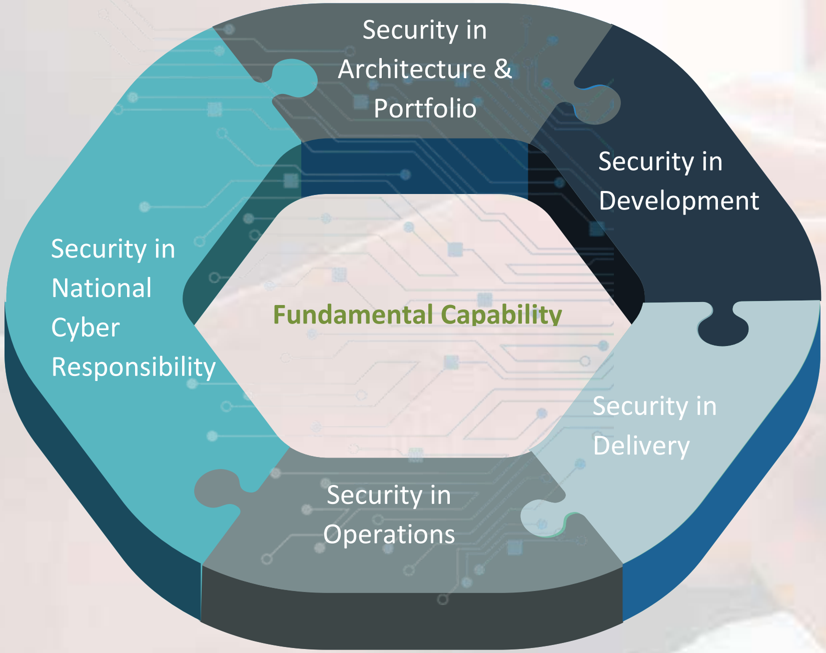
- **Security in Delivery:** Security in Delivery refers to the measures taken to protect data and services during transformation and delivery. Such measures include secure encryption, tracking and monitoring systems, and personnel background checks. Delivery security aims to ensure that service/data 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:



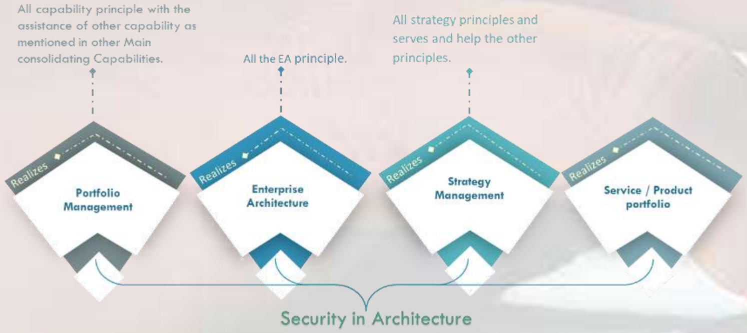
The ensuing exposition presents a comprehensive overview of the capabilities, taking into account the salient features of each while enlisting the related sub-capabilities of each of the principal capabilities. It is intended to offer a concise and lucid summary of the capabilities and sub-capabilities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

## 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.

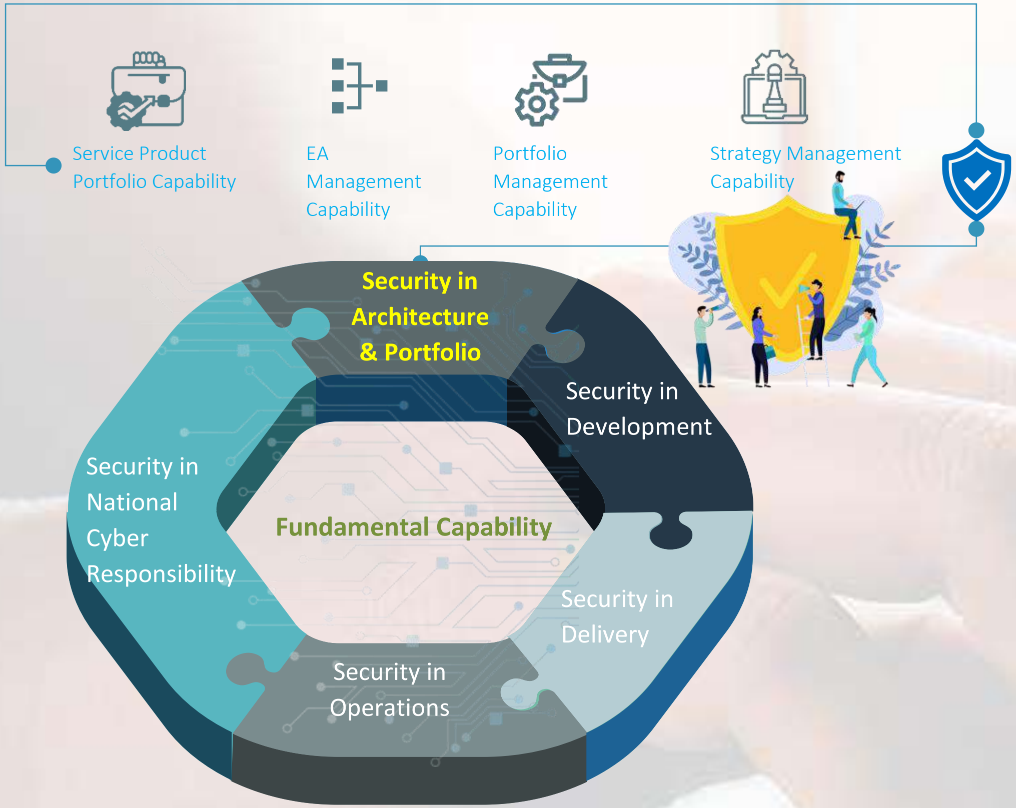
To have this consolidating capability, each entity must have the following underlying main capability developed, maintained, and activated at the appropriate maturity level:


All capability principle with the assistance of other capability as mentioned in other Main consolidating Capabilities.
All the EA principle.
All strategy principles and serves and help the other principles.
Realizes
Portfolio Management
Realizes
Enterprise Architecture
Realizes
Strategy Management
Realizes
Service / Product portfolio
Security in Architecture

- **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, the cyber risk would be considered at an early stage to ensure pro-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 View

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.


Service Product Portfolio Capability
EA Management Capability
Portfolio Management Capability
Strategy Management Capability
Security in Architecture & Portfolio
Security in Development
Security in National Cyber Responsibility
Fundamental Capability
Security in Delivery
Security in Operations

- This capability consists of the following main capabilities:
  - Strategy Management Capability
  - Enterprise Architecture Management Capability
  - Portfolio Management Capability
  - Product / Services Portfolio Capability

- The capability services as the planning phase or cycle regarding achieving an integrated cyber security and cyber risk management process, Where each entity is direct responsibility for ensuring the execution of the process.

- Each main capability realizes some main principles as below, where each realization may be associated with the other capability in a collaboration manner :
  - The Strategy Management Capability realizes all strategy principles and serves and helps the other principles.
  - The Enterprise Architecture Capability realizes all the enterprise-driven principles.
  - Portfolio management. The Product/Service portfolio realizes the all-capability principle with the assistance of other capabilities, as mentioned in other Main consolidating Capabilities.

- All the Sb-main capabilities are formed by utilizing, developing, and maintaining underlying functions that may consist of Tools, People, Technology, and information or data.

- Each Main Sub Capability serves the other with the importance of the strategy and EA interrelation.

- The full capability is connected to the rest of the framework capabilities in terms of serving wise and flow of information.

- The Main Data output from the planning eco-cycle as part of the holistic cyber data models are :

  -Cybersecurity strategy
  -Cybersecurity Portfolio
  -EA & DNA models
  -Cybersecurity Architecture
  -Product/ Service Security Road Map

- This capability is part of influencing the General Philosophy of the Jordan National Cyber Security Center.

## Benefits of the Capability of Security in Architecture Portfolio

The strategy to portfolio functions describes a prescriptive framework of required functional components and information objects that entities can use to control better strategy alignment to the investment and product/services portfolio functional components.

The following are the primary advantages of utilizing the strategy to portfolio functions:

Business Benefits

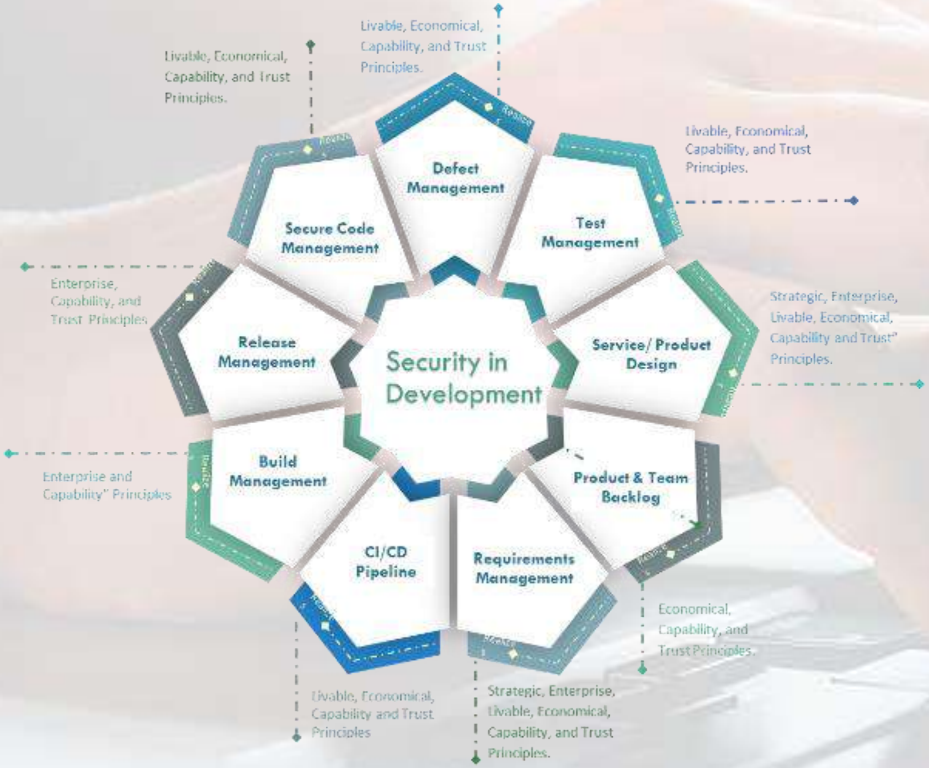
- A holistic portfolio view encompassing the functional components of strategy, enterprise architecture, portfolio backlog, proposal, and product portfolio.
- Portfolio decisions made in accordance with business priorities.
- Tracking the lifecycle of a product across conceptual, logical, and physical domains.
- Rebalance investments in response to strategic and operational demand.
- Prioritized investment based on all portfolio aspects, such as cost/value analysis, architectural implications, product/service roadmap, business priorities, and feasibility.
- Effective communication with business stakeholders via scope agreements and roadmaps.

## 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:


Security in Development
Defect Management
Livable, Economical, Capability, and Trust Principles.
Test Management
Livable, Fconomical, Capability, and Trust Principles.
Service/ Product Design
Strategic, Enterprise, Livable, Economical, Capability and Trust" Principles.
Product & Team Backlog
Economical, Capability, and Trust Principles.
Requirements Management
Strategic, Enterprise, Livable, Economical, Capability, and Trust Principles.
CI/CD Pipeline
Livable, Economical, Capability and Trust Principles
Build Management
Enterprise and Capability" Principles
Release Management
Enterprise, Capability, and Trust Principles
Secure Code Management
Livable, Economical, Capability, and Trust Principles.

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.

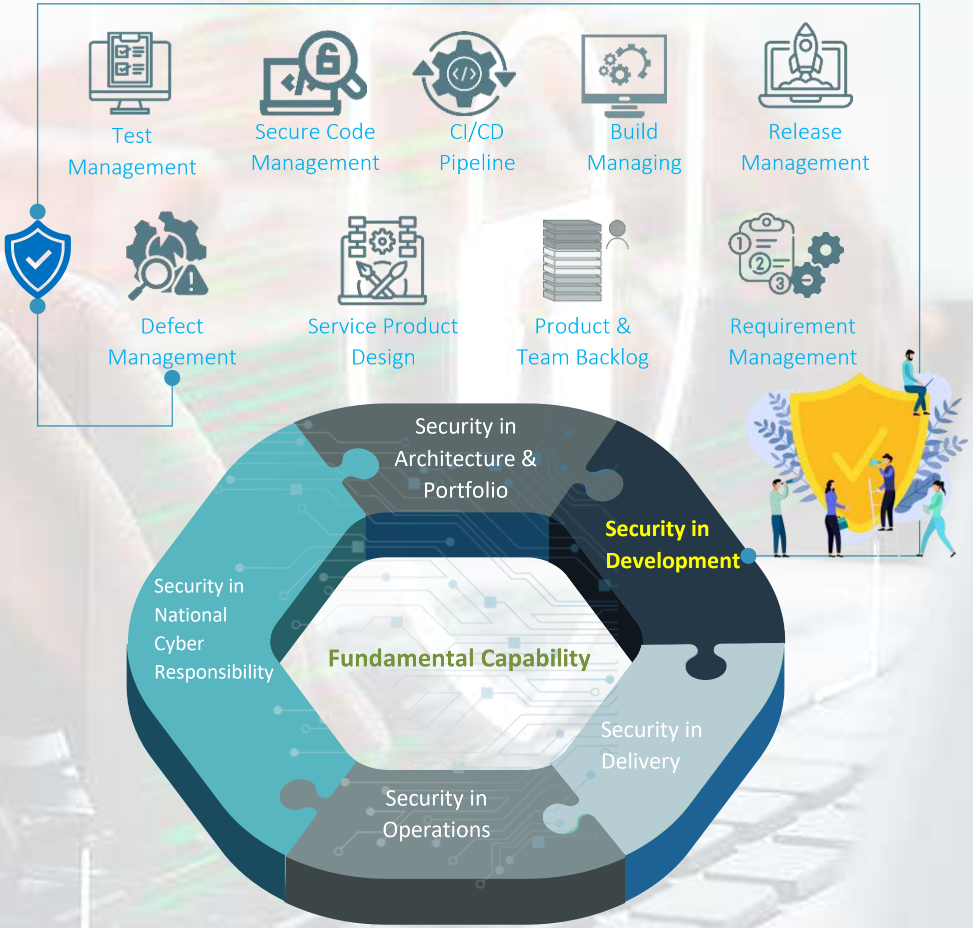
7. **Defect Management Capability**: security in development is the process of identifying, tracking, and resolving security-related defects in the software system. It includes capabilities such as security defect tracking, resolution, root cause analysis, reporting, and vulnerability management.

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.



- This capability is made up of the nine previously mentioned capabilities, which are known as Requirements to Deploy Functions.
- The capability services serve as the foundation for achieving an integrated cyber security and cyber risk management process, with each entity directly responsible for ensuring the process's execution.
- Each main capability realizes some key principles, which are listed below, and each realization can be linked to the other capability in a collaborative manner:
    - The Requirements Management Capability realizes each of all “Strategic, Enterprise, Livable, Economical, Capability and Trust” Principles.
    - The Product & Team Backlog Capability realizes all “Economical, Capability, and Trust” Principles.
    - The Service/ Product Design Capability realizes all “Strategic, Enterprise, Livable, Economical, Capability and Trust” Principles.
    - The Secure Code Management Capability realizes all “Livable, Economical, Capability and Trust” Principles.
    - The Test Management Capability realizes all “Livable, Economical, Capability and Trust” Principles.
    - The CI/CD Pipeline Capability realizes all “Livable, Economical, Capability and Trust” Principles.
    - The Defect Management Capability realizes all “Livable, Economical, Capability and Trust” Principles.
    - The Build Management Capability realizes all “Enterprise and Capability” Principles.
    - The Release Management Capability realizes all “Enterprise, Capability and Trust” Principles.
- All the sub-main capabilities are formed by utilizing, developing, and maintaining underlying functions that may consist of Tools, People, Technology, and information or data.
- The Main/ Sub Capabilities are mutually beneficial.
- The whole capability is for sure connected to the rest of the framework capabilities in terms of serving wise and flow of information.
- The Main Data output from the building eco-cycle as part of the holistic cyber data models are:
    - Requirements Management
    - Service / Product Design
    - Test Management
    - Product & Team Backlog
    - Secure Code Management
    - Build Management
- This capability is part of influencing the General Philosophy of the Jordan National Cyber Security Center.

## Business Benefits of the Capability of Security in Development

The requirement to deploy describes a prescriptive framework of required functional components, integrations, and data objects to enable entities to deliver better value more quickly and safely while lowering costs and increasing product team productivity.

The primary benefits of using the requirement to deploy functions are as follows:

Business Benefits

- Increasing the delivery speed of Product Backlog Items.
- Increased availability of new product releases.
- Increased testing coverage and traceability lead to higher change success rates and lower security risks.
- Traceability and transparency from requirement and/or backlog item to Product Release.
- Security and compliance reduce risk by design. Interoperability, communication, and collaboration among stakeholders and teams involved have all improved (including external vendors).
- Service component reuse has become the norm as product development and delivery have become so standardized..

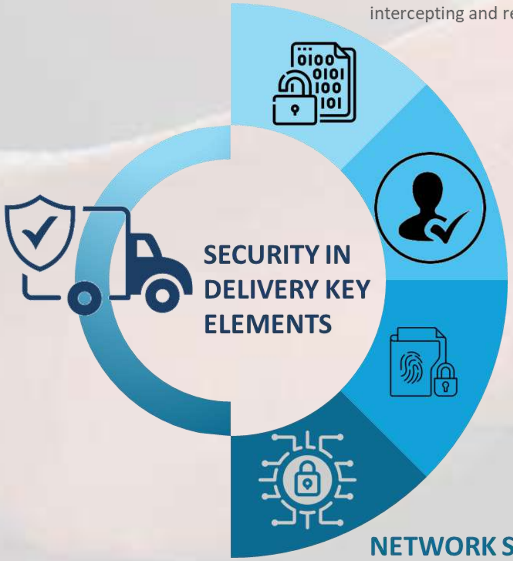
- The delivery of product backlog items has been accelerated (e.g., new features or resolving defects or problems)
- Increasing the rate at which new products are introduced: Using the same automatable architecture across teams can improve release frequency predictability and manageability (and, by extension, standardized tools for the most automatable parts of the development and release chains). By ensuring that the Product Release includes all the content required for automated instantiation, the Requirement to Deploy functional and data models provides an architecture capable of reducing the time from committed code to live systems to zero. That will Increase the rate at which new products are introduced.
- More complete and traceable testing capability should result in higher change success rates and reduced security risks.
- End-to-end transparency and traceability from requirement and/or backlog item to Product Release.
- Reducing the risk due to security and compliance by design, and this is to the maintaining process of the association between entity policy and requirement data objects throughout the product lifecycle by the requirement to deploy functions. This persistent traceability enables designers to ensure that all non-functional requirements are accounted for so that products are designed per standards and policies from sources such as security management, governance, risk, & compliance, legal & regulatory, enterprise architecture, and financial management.
- Improved interoperability, communication, and collaboration among involved stakeholders and teams (including external vendors): Applications and services can be sourced or developed in collaboration with a variety of parties, each of which uses its own processes and tooling. The requirement to deploy functional criteria defines an interoperability standard that allows entities to enforce a consistent, standardized description of planned activities as well as function and data interoperability.

## 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.

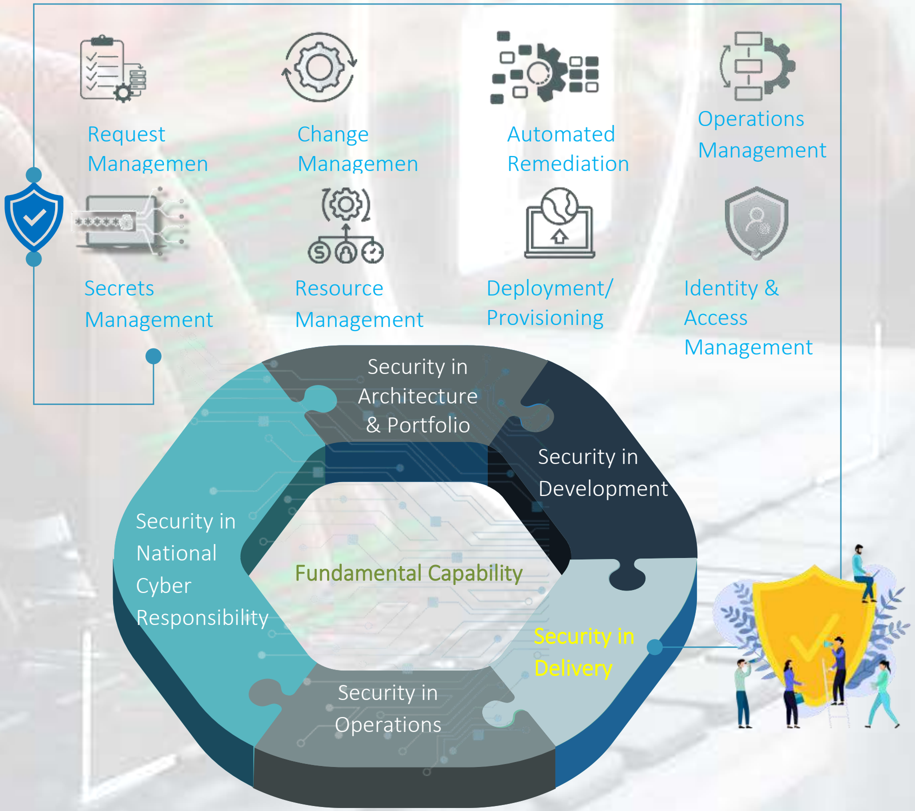
**NETWORK SECURITY**

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.



- The capabilities are divided into main capabilities, with each realization being associated with the other capability in a collaborative manner; a summary of these main capabilities is provided below:
  - Resource Management Capability realizes each of: Capability Principles, Enterprise Principles, and Trust Principles.
  - Automated Remediation realizes Liveable Principles
  - Request Management realizes each of: Economic Principles, Enterprise Principles, and Trust Principles.
  - Change Management realizes each of: Capability Principles, Enterprise Principles, Livable Principles, Economical Principles, and Trust Principles.
  - Identity & Access Management realizes each of: Capability Principles, Enterprise Principles, Livable Principles, Economical Principles, and Trust Principles.
  - Deployment/Provisioning realize Capability Principles, Livable Principles, and Trust Principles.
  - Secrets Management realizes Trust Principles, Capability Principles, and Livable Principles.
  - Operations Management realizes Trust Principles, Capability Principles, and Livable Principles.
- All the related capabilities are formed by utilizing, developing, and maintaining underlying functions that may consist of Tools, People, Technology, and information or data.
- Each Main Sub Capability serves the other with the importance of the strategy and enterprise architecture interrelation.
- The full capability is connected to the rest of the framework capabilities in terms of serving wise and flow of information.
- The main data output from the planning eco-cycle as part of the holistic cyber data models are :
  - Request Register.
  - Identity & Access Management.
  - Secrets Management Policy.
  - Resource Management Plan.
  - Change Register.
  - Deployment/Provisioning.
  - Technical Operations Information.
  - Remediation Plan.
- Capability influences the General Philosophy of the Jordan Cyber Security Center.

## Benefits to the Capability of Security in Delivery

Benefits
Data Protection
Comply With Various Regulations and Standards
Reputation
Cost effective

- **Data Protection -** Security in delivery ensures that the data being transmitted is protected from unauthorized access, alteration, or theft. This helps to prevent data breaches and the loss of sensitive information.
- **Compliance -** Security in delivery helps entities to comply with various regulations and standards, such as HIPAA and PCI-DSS, which require secure data transmission.
- **Reputation Protection -** Entities that implement security in delivery can protect their reputation by demonstrating to customers and partners that they take the security of their data seriously.
- **Cost-effective -** Implementing security in delivery can ultimately save entities money by reducing the risk of data breaches, which can be costly in terms of both financial and reputational damage.

## Security in Operations

Security in operations refers to the practices and processes that aim to protect an entity's services, 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.

The security in operations functions also provides a comprehensive overview of the digital operations business and the services provided by an Operations team, including security operations. This point of view provides an understanding of the interdependence of its many domains, as well as responsiveness to business requests and requirements.

One of the main objectives of security operations is to detect security incidents in operations and respond to them in a timely and effective manner, all while continuously improving the entities' overall security situation. Continuous monitoring and analysis of security data, as well as regular testing and updating of security controls, are required. Furthermore, security operations teams must have clear incident response plans and conduct regular exercises to ensure operations' incident response capabilities are effective.

Security in operations functions brings together operations functions to improve services and efficiencies, thereby lowering risk.

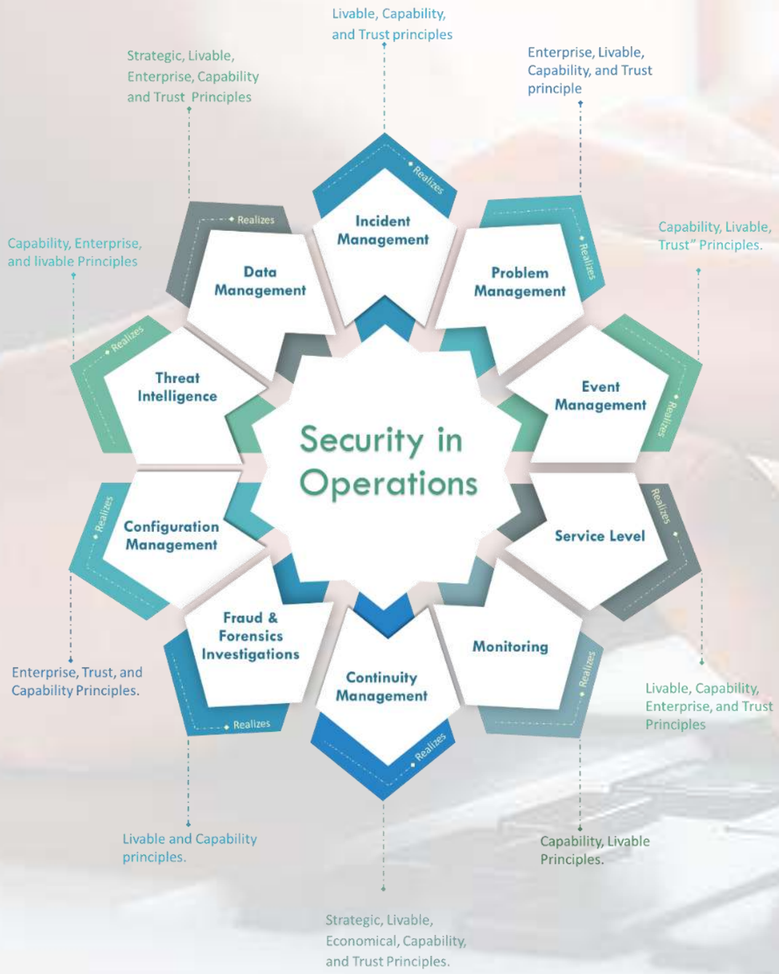
Security operations are a collection of key capabilities designed to protect an entity, service, networks, and systems. Incident response, threat intelligence, and vulnerability scanning are examples of these activities.

These activities are listed below, along with a brief description of each.

- **Incident Response Capability**: This refers to the process of identifying, containing, and mitigating the effects of a security incident. Detecting, analyzing, and responding to security incidents is typically the responsibility of a team of security professionals. They may use a variety of tools and techniques to identify potential threats, such as intrusion detection systems, security information and event management (SIEM) systems, and network analysis tools.
- **Threat Intelligence Capability**: it is the gathering and analysis of information about potential threats to an entity's assets. This data can be used to discover new vulnerabilities, track the activities of known attackers, and devise mitigation strategies for potential attacks. Entities can gather threat intelligence from various sources, including open-source information, industry groups, and government agencies.
- **Monitoring Capability**: Monitoring for potential threats is also an important aspect of operational security. This can include monitoring network traffic, logging system events, and detecting and responding to potential threats using security tools such as intrusion detection and prevention systems.
- **Vulnerability Scanning Capability:** This major key identifies, assesses, and mitigates vulnerabilities in an entity's assets, networks, and systems. This includes scanning for vulnerabilities regularly, identifying and prioritizing the most critical ones, and implementing remediation measures.
- **Problem Management Capability:** Majorly, it aids in identifying, analyzing, and resolving security-related issues that may arise within an entity to reduce the risk of future occurrences. It is critical to have a process in place to identify, diagnose, and fix security vulnerabilities or incidents.
- **Configuration Management Capability:** This assists in ensuring the security of entities' technologies, IT, OT, IoT, and ET systems and infrastructure, as well as the proper control and tracking of changes to those systems. This can include putting in place security controls, such as access controls, to safeguard sensitive data and resources.
- **Continuity Management Capability**: it is critical for ensuring the entity's ability to continue operations in the event of a security incident or disruption. This can include creating incident response plans and procedures and regularly testing and training to ensure the plans are effective.
- **Data Management Capability:** The process of protecting and managing sensitive data, such as personal information, financial data, and proprietary information, is known as data management. This includes putting in place data-protection

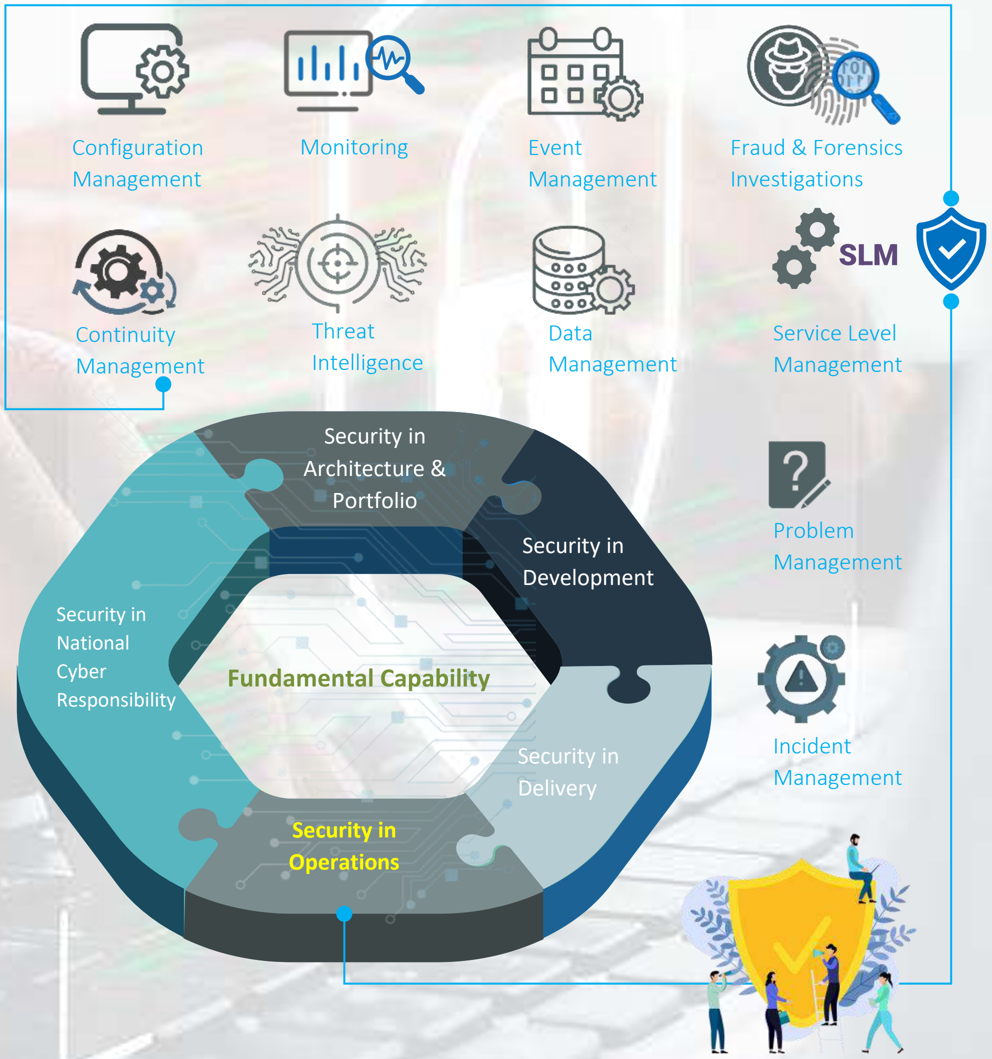
safeguards such as identification, decomposition, classification, encryption, policy development, and data management procedures.

- **Service Level Management Capability**: The process of ensuring that an entity's IT, OT, IoT, IIoT, and ET systems and services meet the needs of its customers and stakeholders is known as service level management. Entities can ensure that their systems meet the required standards and that customers and stakeholders are satisfied with the service provided by having clear service level agreements (SLA) and monitoring the performance of these systems. This is an example of monitoring and reporting on system availability, performance, and security.


Livable, Capability, and Trust principles
Strategic, Livable, Enterprise, Capability and Trust Principles
Enterprise, Livable, Capability, and Trust principle
Capability, Enterprise, and livable Principles
Capability, Livable, Trust" Principles.
Security in Operations
Incident Management
Data Management
Problem Management
Threat Intelligence
Event Management
Configuration Management
Service Level
Fraud & Forensics Investigations
Continuity Management
Monitoring
Realizes
Enterprise, Trust, and Capability Principles.
Livable, Capability, Enterprise, and Trust Principles
Livable and Capability principles.
Capability, Livable Principles.
Strategic, Livable, Economical, Capability, and Trust Principles.

## 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.



- This main capability contains many other capabilities, including:

  - Incident Management Capability
  - Problem Management Capability
  - Event Management Capability
  - Monitoring Capability
  - Continuity Management Capability
  - Fraud & Forensics Investigations Capability
  - Configuration Management Capability
  - Threat Intelligence Capability
  - Data Management Capability
  - Service Level Management Capability

- The operation cycle's "Run" phase, also known as security in operations functions, provides a framework for the secure operation of digital products and services, ensuring that all running systems are within defined boundaries and managed securely, with a comprehensive overview of business operations and security operations to provide an understanding of relationships and responsiveness to business needs.

  - Each main capability realizes some main principles as below, where each realization may be associated with the other capability in a collaboration manner:

    - The Incident Management Capability realizes all “Livable, Capability, and Trust “principles.
    - The Problem Management Capability realizes all the “Enterprise, Livable, Capability and Trust” principles.
    - The Event Management Capability realizes all the “Capability, Livable, Trust” Principles.
    - The Monitoring Capability realizes all the “Capability and Livable” principles.
    - The Continuity Management Capability realizes all the “Strategic, Livable, Economic, Capability and Trust” Principles.
    - Fraud & Forensics Investigations Capability realizes all the “Livable and Capability “principles.
    - Configuration Management Capability realizes all the “Enterprise, Trust, and Capability” Principles.
    - Threat Intelligence Capability realizes all the “Capability, Enterprise, and livable” Principles.
    - Data Management Capability realizes all the “Strategic, Livable, Enterprise, Capability and Trust” Principles.
    - Service Level Management Capability realizes all the “Livable, Capability, Enterprise and Trust” Principles.

- All the sub-capabilities are formed by utilizing, developing, and maintaining underlying functions, which may include Tools, People, Technology, and information or data.

- Each main sub-capability complements the others.

- In terms of serving and information flow, the entire capability is unquestionably linked to the rest of the framework's capabilities.

- The Main Data output from the planning eco-cycle as part of the holistic cyber data models are:

  - Cybersecurity Incident Data
  - Cybersecurity Problem Register
  - Monitoring Information
  - Backup Policy
  - Service Level Policy
  - Cybersecurity Event Register
  - Continuity Plan
  - Configuration & Asset Data
  - Threat Intelligence Reports

- This main capability is part of influencing the General Philosophy of the Jordan Cyber Security Center.

## Benefits to the Capability of Security in Operations

The key benefits for security in operations are:

Benefits

- Increase Efficiency and Reduce Cost.
- Reduce Risk.
- Continuous Service Improvement.
- Other Benefits of Security in Operations.

Increase efficiency and reduce cost by:

- Centralized Event Management for faster analysis.
- Automation between and across business functions.
- Knowledge management and self-service linkage.
- Improving the speed at which issues with an Actual Product Instance are identified.
- Driving operating/service level targets.
- Improving the speed at which issues with an Actual Product Instance are proactively detected.

## Fundamental Capabilities

To effectively safeguard services, systems, networks, and data from unauthorized access, misuse, and malicious attacks, entities and individuals must possess fundamental capabilities in cybersecurity. These capabilities are crucial for ensuring the confidentiality, integrity, availability, and safety of information and services, which are the four primary pillars of information security. To provide a better overview, the following is a list of these fundamental capabilities with a brief of each.

- One of the most important fundamental capabilities in cybersecurity is **Policy Management Capability** Which refers to the process of creating, implementing, and maintaining policies, hierarchy, and procedures that govern an entity's security practices. These policies and procedures are designed to ensure that the entity's information assets are protected and that the entity is in compliance with relevant laws, regulations, and industry standards.

- Another fundamental capability in cybersecurity is **Risk and Compliance Management Capability**, which is the process of identifying, measuring, and prioritizing potential threats to an entity and taking steps to minimize or eliminate those risks. It also involves ensuring that the entity is in compliance with all relevant laws, regulations, and industry standards.

- **Audit Management Capability,** this Capability is the process of evaluating entities' services, information and technology systems, processes, and controls to ensure that they are operating effectively and efficiently and that they are in compliance with applicable laws, regulations, and industry standards. Audit management is a critical component of risk and compliance management.

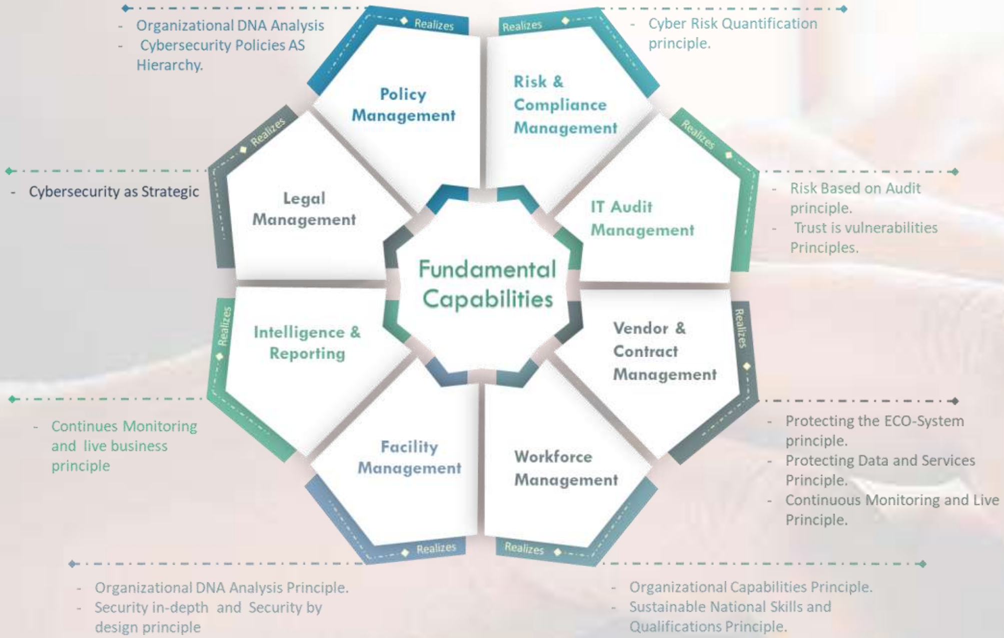
- **Vendor and Contract Management Capability** refers to the process of managing relationships with external vendors and the contracts and agreements that govern these relationships. This process involves identifying and measuring the risks of selecting vendors, managing the procurement process, and overseeing the performance of vendors and the fulfillment of their contracts according to the entity's Cybersecurity standards.

- **Workforce Management Capability**, which is the process of coordinating and optimizing the activities of employees within an entity. This includes scheduling, forecasting, analyzing workforce data, security checks, hiring, training employees, and setting goals and priorities to improve efficiency and productivity. Workforce management is typically concerned with ensuring that an entity has the right number of employees with the right skills in the right place at the right time to meet the business's needs.

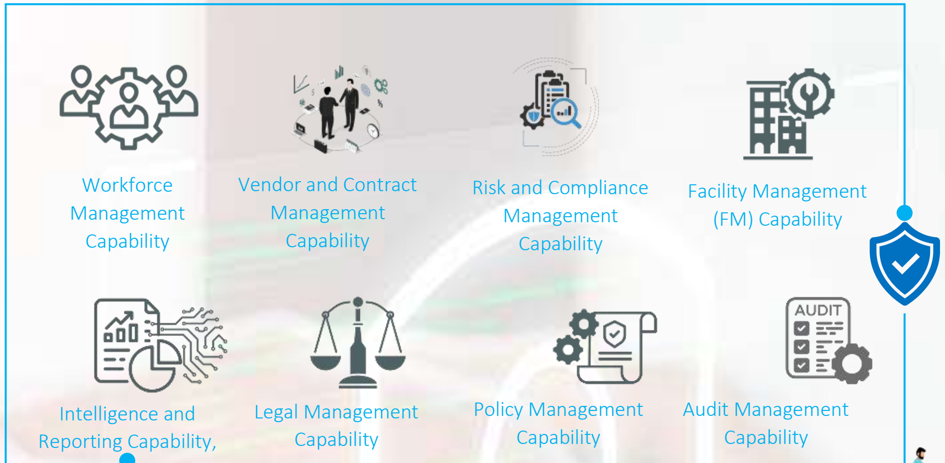
- **Legal Management Capability,** defined as the process of managing the legal affairs and risks of an entity. This can include tasks such as reviewing and drafting legal documents, providing legal advice, managing litigation and disputes, and ensuring compliance with laws and regulations. The goal of legal management is to protect entities' interests and assets, minimize legal risk, and ensure compliance with laws and regulations that apply to the entity's operations and activities.

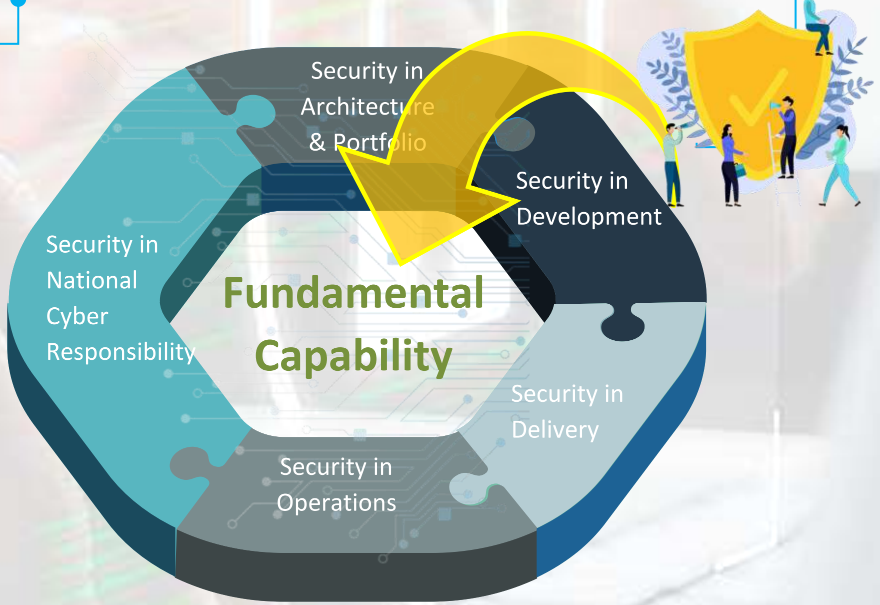
- **Facility Management (FM) Capability,** defined as the process of managing and maintaining entities' buildings, equipment, and grounds, as well as the services that support the core business of an entity. It is an interdisciplinary field that includes a wide range of activities, such as maintenance, security, cleaning, energy management, safety, and health. The goal of facility management is to ensure that the entity's physical assets and infrastructure are well-maintained, safe, and secure and that they support the entity's operations and objectives.

- Finally, **Intelligence and Reporting Capability,** this capability refers to the process of gathering, analyzing, and disseminating information about cyber threats, vulnerabilities, and attacks that are relevant to an entity's information systems and networks. This can include tasks such as monitoring for malicious activity on the entities networks, analyzing log data and threat intelligence, and identifying patterns and trends that can indicate a potential cyber attack.


- Organizational DNA Analysis
- Cybersecurity Policies AS Hierarchy.
Realizes
Policy Management
Realizes
Risk & Compliance Management
- Cyber Risk Quantification principle.
- Cybersecurity as Strategic
Realizes
Legal Management
Realizes
IT Audit Management
- Risk Based on Audit principle.
- Trust is vulnerabilities Principles.
Fundamental Capabilities
Realizes
Intelligence & Reporting
Realizes
Vendor & Contract Management
- Continues Monitoring and live business principle
Facility Management
Workforce Management
- Protecting the ECO-System principle.
- Protecting Data and Services Principle.
- Continuous Monitoring and Live Principle.
Realizes
Realizes
- Organizational DNA Analysis Principle.
- Security in-depth and Security by design principle
- Organizational Capabilities Principle.
- Sustainable National Skills and Qualifications Principle.

## A Comprehensive Overview


Workforce Management Capability
Vendor and Contract Management Capability
Risk and Compliance Management Capability
Facility Management (FM) Capability
AUDIT
Intelligence and Reporting Capability,
Legal Management Capability
Policy Management Capability
Audit Management Capability



- The capability services as a supporting phase regarding achieving an integrated cyber security and cyber risk management process where each entity is directed to ensure the execution of the process.
- Each main capability realizes some main principles as below, where each realization may be associated with the other capability in a collaboration manner:

- Policy Management Capability realizes two Principles entity DNA Analysis & Cybersecurity Policies AS Hierarchy.

- Risk and Compliance Management Capability realizes all livable principles and realizes the Cyber Risk Quantification principle.

- IT Audit Management Capability realizes Risk Based Audit principle, and Trust is a  vulnerabilities Principles.

- Vendor and contract Management realize protecting the ECO-System principle, protecting Data and Services principle, and Continuous Monitoring and Live principle.

- Workforce Management Capability Realize entity Capabilities Principle and Sustainable National Skills and Qualification Principle.

- Facility Management realizes entity DNA Analysis Principle and Security in depth and security by design principle.

- Intelligence & Reporting Capability realize Continues Monitoring and live business principle.

- Legal Management capability realizes cyber security as a strategic imperative.

▪ All the sub-main capabilities are formed by utilizing, developing, and maintaining underlying enabler functions that may consist of tools, people, technology, and information or data where some technology tools are mentioned in the architecture.

▪ The full capability is connected to the rest of the framework capabilities in terms of serving wise and flow of information.

▪ The primary data output from the planning eco-cycle as part of the holistic cyber data models are :

  - Cybersecurity Policy
  - Cybersecurity Audit
  - Cybersecurity Risk
  - Facility Management
  - Cybersecurity vendor
  - Intelligence & Reporting
  - Workforce Management

▪ The capability is part of influencing the general philosophy of the Jordan Cyber Security Center.

### Benefits to the Fundamental Capabilities

Benefits

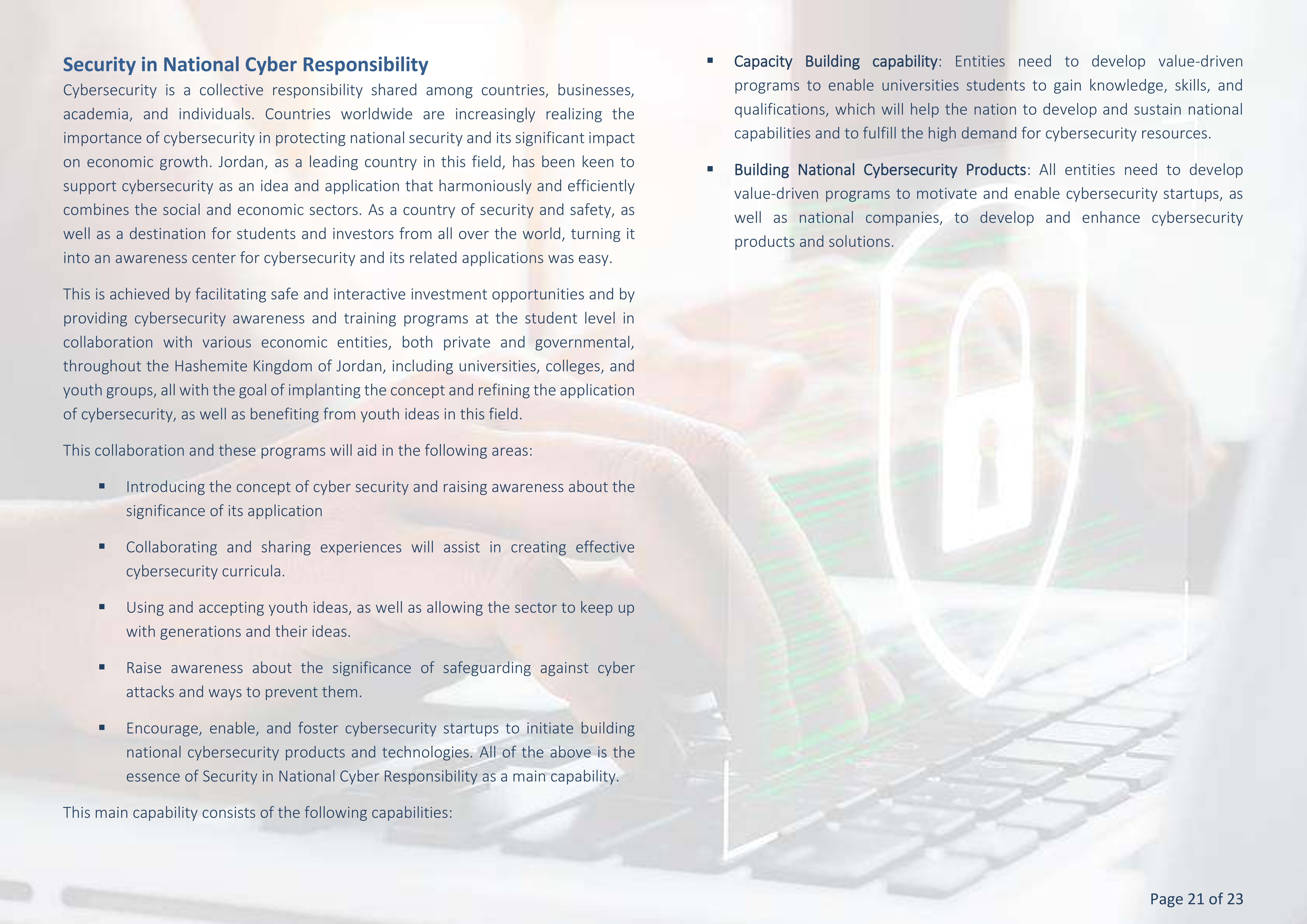
- They provide a basic level of protection for an organization's assets and data.
- They help to identify and mitigate cyber risks.
- They support compliance with regulatory requirements.
- They improve overall security posture and resilience.
- They can help to prevent cybercrime and protect intellectual property.
- They can reduce costs associated with security breaches.

▪ **They provide a basic level of protection for an entity's assets and data:** Without basic security measures, an entity's data and information may be vulnerable to cyber-attacks; that is why one of the most important benefits of foundational capabilities from cyber attacks is providing essential information protection.

▪ **They help to identify and mitigate cyber risks:** Without incident response and security awareness training, an entity may be unable to detect and respond to cyber threats effectively, and having the basic capability will solve such a problem.

▪ **They support compliance with regulatory requirements:** Many industries are subject to regulations that necessitate specific security measures. Without foundational capabilities, an entity may be out of compliance and subject to fines or penalties.

▪ They improve overall security posture and resilience.



## Security in National Cyber Responsibility

Cybersecurity is a collective responsibility shared among 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. Jordan, as a leading country in this field, has been keen to support cybersecurity as an idea and application that harmoniously and efficiently combines the social and economic sectors. As a country of security and safety, as well as a destination for students and investors from all over the world, turning it into an awareness center for cybersecurity and its related applications was easy.

This is achieved by facilitating safe and interactive investment opportunities and by providing cybersecurity awareness and training programs at the student level in collaboration with various economic entities, both private and governmental, throughout the Hashemite Kingdom of Jordan, including universities, colleges, and youth groups, all with the goal of implanting the concept and refining the application of cybersecurity, as well as benefiting from youth ideas in this field.

This collaboration and these programs will aid in the following areas:

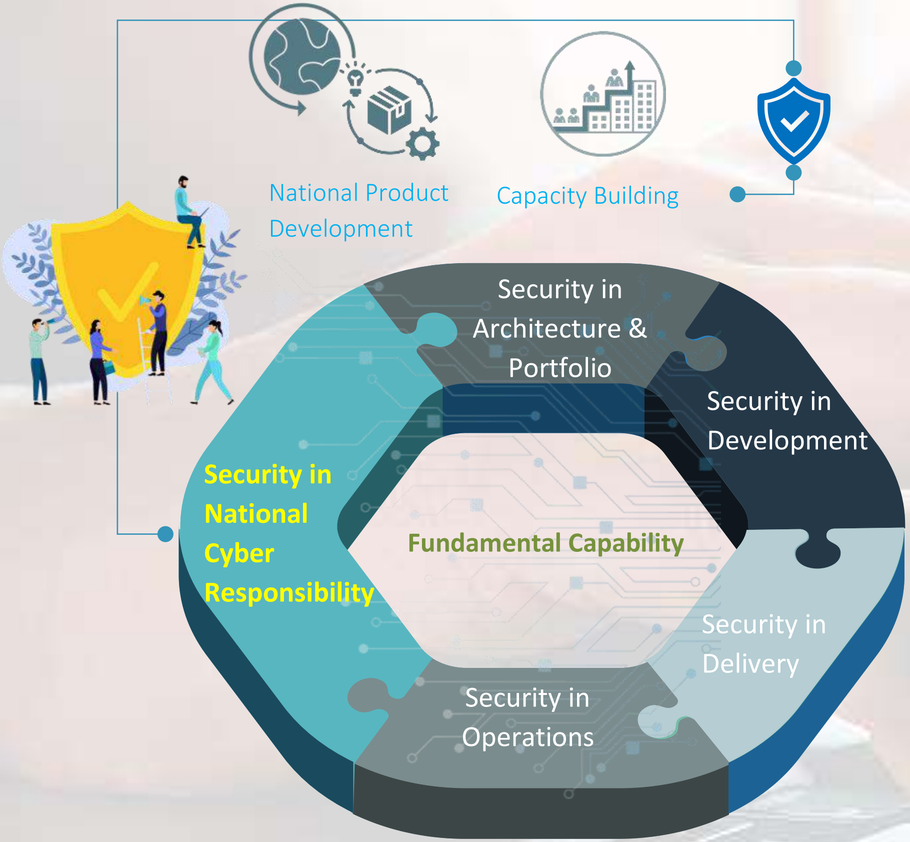
- Introducing the concept of cyber security and raising awareness about the significance of its application
- Collaborating and sharing experiences will assist in creating effective cybersecurity curricula.
- Using and accepting youth ideas, as well as allowing the sector to keep up with generations and their ideas.
- Raise awareness about the significance of safeguarding against cyber attacks and ways to prevent them.
- Encourage, enable, and foster cybersecurity startups to initiate building national cybersecurity products and technologies. All of the above is the essence of Security in National Cyber Responsibility as a main capability.

This main capability consists of the following capabilities:

- **Capacity Building capability**: Entities need to develop value-driven programs to enable universities students to gain knowledge, skills, and qualifications, which will help the nation to develop and sustain national capabilities and to fulfill the high demand for cybersecurity resources.
- **Building National Cybersecurity Products**: All entities need to develop value-driven programs to motivate and enable cybersecurity startups, as well as national companies, to develop and enhance cybersecurity products and solutions.

## 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.


National Product Development
Capacity Building
Security in Architecture & Portfolio
Security in Development
Security in National Cyber Responsibility
Fundamental Capability
Security in Delivery
Security in Operations

- The capability services as the National Responsibilities phase for achieving an integrated cyber security and cyber risk management process in which each entity is directly responsible for ensuring process execution.
- Each Capability may be associated with the other capability collaboratively, for example.
  - Capacity Building capability highlights the principle of entityal capabilities and the principle of sustainable national skills and qualifications.
  - National products capability realizes national cybersecurity products and technologies principle.
- All sub-capabilities are created by utilizing, developing, and maintaining underlying enabler functions such as Tools, People, Technology, and information or data where technology tools are mentioned in the architecture.
- The full capability is inextricably linked to the rest of the framework capabilities regarding serving and information flow.
- The Main Data output from the planning eco-cycle as part of the holistic cyber data models is Cybersecurity Training and awareness and National Cybersecurity vendors.
- Capability is part of influencing the General Philosophy of the Jordan Cyber Security Center.

## Benefits of the Main Capability of Security in National Cyber Responsibility

Benefits

- Increased availability of highly skilled cybersecurity professionals.
- Attract international investments.
- Encourage entrepreneurship and innovation.
- Cooperate with educational authorities to develop curricula on cybersecurity.

- Increased availability of highly skilled cybersecurity professionals can lead to more secure and stable economic systems and promote economic growth and innovation by providing businesses with the tools and resources they need to protect their digital assets, reducing the lack of a skilled workforce in the cybersecurity field.
- Attract international investment and boost trust in the country's digital infrastructure, which can significantly attract foreign investment.
- Encourage entrepreneurship and innovation by giving students and professionals the necessary skills and knowledge to start cybersecurity-focused businesses. This will have an economic impact by providing unlimited research and development that increase the opportunity to capitalize on the accelerated digital transformation cycle, achieving economic growth. Interaction between governmental and private entities with educational institutions will help to alleviate this problem by providing funds for research and adopting related youth ideas.