CYBERSECURITY FRAMEWORK

CYBERSECURITY FRAMEWORK

- **A cybersecurity framework** is a structured set of guidelines and best practices designed to help organizations manage and mitigate Cybersecurity risks associated with their information and technology systems.

CYBERSECURITY FRAMEWORK

- **The Purpose of the Framework**
- Offering a holistic strategy for defending against cyber threats.
- Identify potential vulnerabilities.
- Protect critical assets.
- Detect anomalies or breaches.
- Respond to threats promptly.
- Recover effectively after an incident.

CYBERSECURITY FRAMEWORK

- **The Role of Cybersecurity Frameworks**
- Ensuring business continuity
- Protecting brand reputation
- Maintaining customer trust
- Meeting regulatory compliance requirements.

NIST CYBERSECURITY FRAMEWORK

- **The National Institute of Standards and Technology (NIST)** is a non-regulatory agency that promotes innovation by advancing measurement science, standards and technology.
- The NIST CSF is flexible enough to integrate with the existing security processes within any organization, in any industry. It provides an excellent starting point for implementing information security and cybersecurity risk management

NIST CYBERSECURITY FRAMEWORK

- **The Three Primary Components :**
- **Core**

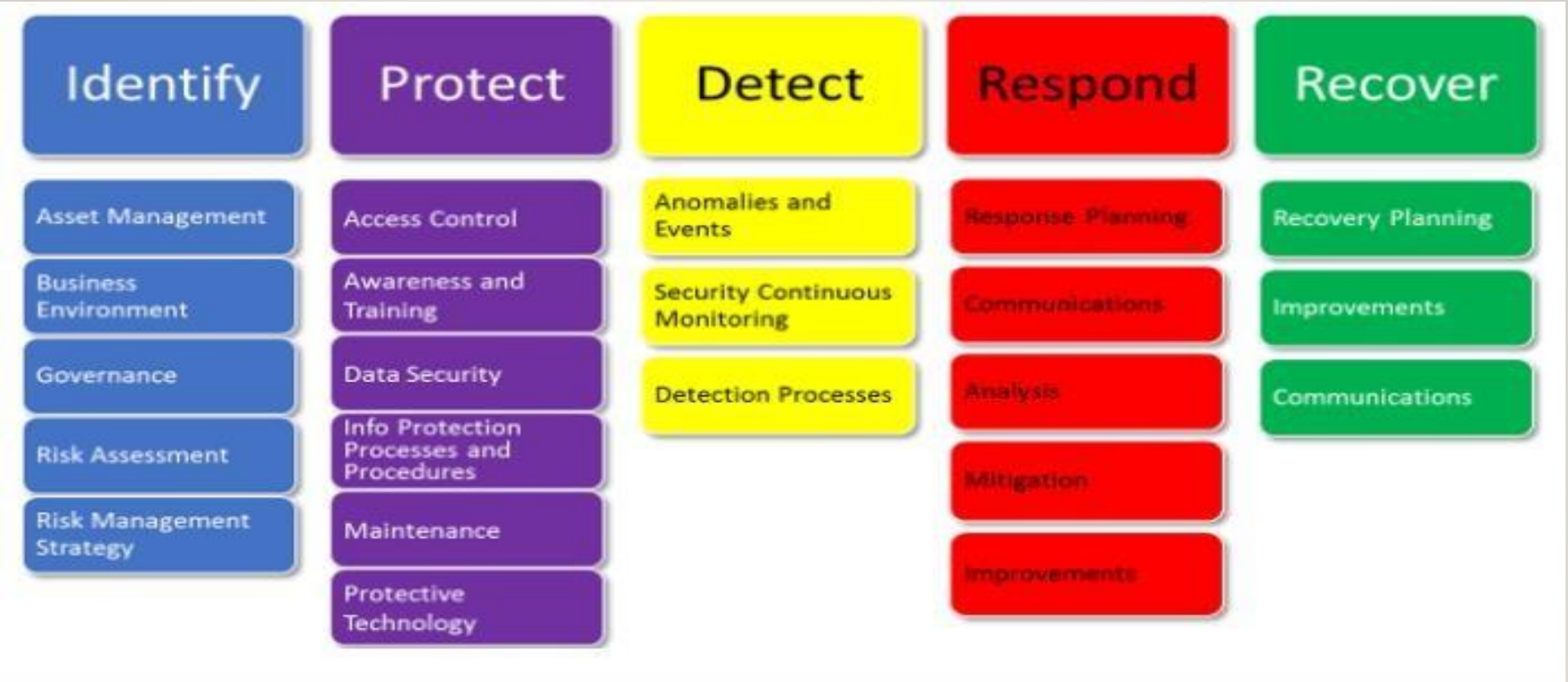
  Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls
- **Profiles**

  Alignment of an organization's requirements and objectives, risk appetite and resources ***using*** the desired outcomes of the Framework Core
- **Implementation Tiers**

  A qualitative measure of organizational cybersecurity risk management practices

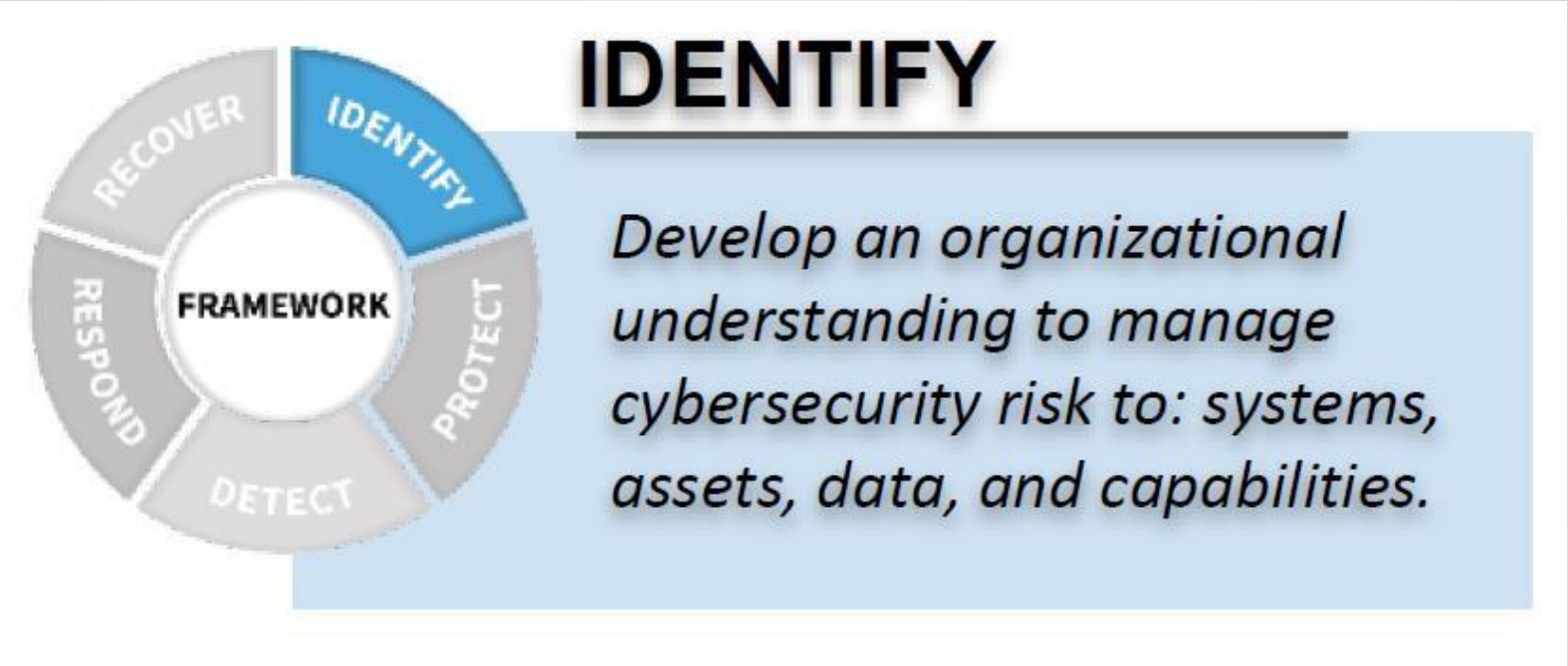
NIST CYBERSECURITY FRAMEWORK

- **The Framework Core:**



NIST CYBERSECURITY FRAMEWORK

- **The Framework Core Structure :**
- **(ID)**



NIST CYBERSECURITY FRAMEWORK

- **ID. Asset Management :**
- The data, personnel, devices, systems, and facilities that

enable the organization to achieve business purposes are identified and managed consistent with their relative importance organizational objectives and the organization's risk strategy.

NIST CYBERSECURITY FRAMEWORK

- **ID. Asset Management :**

1. Physical devices and systems within the organization are inventoried
2. Software platforms and applications within the organization are inventoried
3. Organizational communication and data flows are mapped External information systems are catalogued
4. Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
5. Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

NIST CYBERSECURITY FRAMEWORK

- **ID. Business Environment :**
- The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

NIST CYBERSECURITY FRAMEWORK

- **ID. Business Environment :**

1. The organization's role in the supply chain is identified and communicated.
2. The organization's place in critical infrastructure and its industry sector is identified and communicated.
3. Priorities for organizational mission, objectives, and activities are established and communicated.
4. Dependencies and critical functions for delivery of critical services are established
5. Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery ,normal operations)

NIST CYBERSECURITY FRAMEWORK

- **ID. Governance:**
- The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. .

NIST CYBERSECURITY FRAMEWORK

- **ID. Governance:**

1. Organizational cybersecurity policy is established and communicated
2. Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
3. Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
4. Governance and risk management processes address cybersecurity risks

NIST CYBERSECURITY FRAMEWORK

- **ID. Risk Assessment:**
- The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

NIST CYBERSECURITY FRAMEWORK

- **ID. Risk Assessment:**

1. Asset vulnerabilities are identified and documented
2. Cyber threat intelligence is received from information sharing forums
3. Threats, both internal and external, are identified and documented
4. Potential business impacts and likelihoods are identified
5. Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
6. Risk responses are identified and prioritized

NIST CYBERSECURITY FRAMEWORK

- **ID. Risk Management Strategy :**
- The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

NIST CYBERSECURITY FRAMEWORK

- **ID. Risk Management Strategy:**

1. Risk management processes are established, managed, and agreed to by organizational stakeholders
2. Organizational risk tolerance is determined and clearly expressed
3. The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

CYBERSECURITY RISK MANAGEMENT

- **Cybersecurity risk management** is the process of identifying, prioritizing, managing and monitoring risks to information systems.

- **Why Cybersecurity Risk Management is important?**
- It enables a business to examine its existing cybersecurity risk profile. This informs decisions the security organization will make moving forward in order to reduce the level of risk and address vulnerabilities.
- it helps to bring about situational awareness within a security organization. Simply put, analysts don't know what they don't know. Awareness is the ability to look at all the information available, recognize what's important, and act accordingly.

CYBERSECURITY RISK MANAGEMENT

- **Cybersecurity risk management Process:**
- **Identify The Risk:**
- understanding threats, vulnerabilities, and the consequences of their convergence.

CYBERSECURITY RISK MANAGEMENT

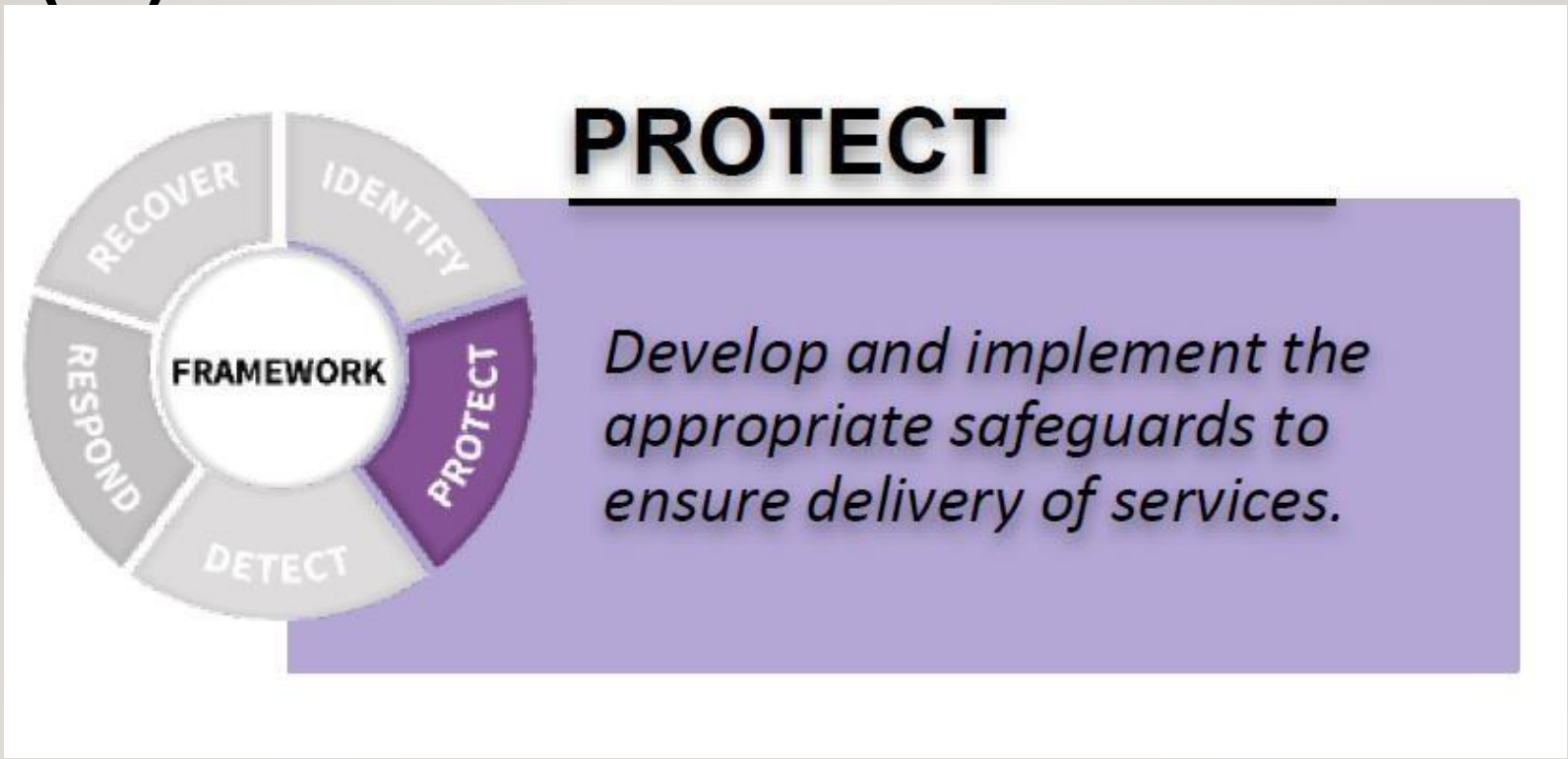
- **Assess The Risk :**
- Name All Assets
- Prioritize the importance of each asset
- Identify all possible threats to your assets
- Identifying all vulnerabilities in your environment
- Determine the likelihood of a threat event occurring
- Conduct and impact analysis to estimate the threat events pectineal consequences and cost impact

CYBERSECURITY RISK MANAGEMENT

- Treat The Risk :
- Risk mitigation.
- Risk remediation.
- Risk transfer.
- Monitor The Risk:
- monitor new security controls to verify that they work as regulatory requirements.

NIST CYBERSECURITY FRAMEWORK

- **The Framework Core Structure :**
- **PROTECT(PR)**



NIST CYBERSECURITY FRAMEWORK

- **PR. Access Control**
- physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions**.**

.

NIST CYBERSECURITY FRAMEWORK

- **PR. Access Control**

1. Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and Processes.
2. Physical access to assets is managed and protected.
3. Remote access is managed.
4. Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

NIST CYBERSECURITY FRAMEWORK

- **PR. Access Control**

5. Network integrity is protected
6. Identities are proofed and bound to credentials and asserted in interactions
7. Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

NIST CYBERSECURITY FRAMEWORK

- **PR. Awareness and Training**
- The organization's Personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity- related duties and responsibilities consistent with related policies, procedures and agreements

.

NIST CYBERSECURITY FRAMEWORK

- **PR. Awareness and Training**

1. All users are informed and trained
2. Privileged users understand their roles and responsibilities
3. Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
4. Senior executives understand their roles and responsibilities
5. Physical and cybersecurity personnel understand their roles and responsibilities

NIST CYBERSECURITY FRAMEWORK

- **PR. Data Security**
- Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information

NIST CYBERSECURITY FRAMEWORK

- **PR. Data Security**

1. Data-at-rest is protected
2. Data-in-transit is protected
3. Assets are formally managed throughout removal, transfers, and disposition.
4. Adequate capacity to ensure availability is maintained
5. Protections against data leaks are implemented

NIST CYBERSECURITY FRAMEWORK

- **PR. Data Security**

6. Integrity checking mechanisms are used to verify software, firmware, and information integrity

7. The development and testing environment(s) are separate from the production environment

8. Integrity checking mechanisms are used to verify hardware integrity

NIST CYBERSECURITY FRAMEWORK

- **PR. Information Protection Processes and Procedures**
- Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

NIST CYBERSECURITY FRAMEWORK

- **PR. Information Protection Processes and Procedures**

1. A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles
2. A System Development Life Cycle to manage systems is implemented
3. Configuration change control processes are in place
4. Backups of information are conducted, maintained, and tested

NIST CYBERSECURITY FRAMEWORK

- **PR. Information Protection Processes and Procedures**

5. Policy and regulations regarding the physical operating environment for organizational assets are met
6. Data is destroyed according to policy
7. Protection processes are improved
8. Effectiveness of protection technologies is shared
9. Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

NIST CYBERSECURITY FRAMEWORK

- **PR. Information Protection Processes and Procedures**

10. Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
11. Response and recovery plans are tested
12. Cybersecurity is included in human resources practices (e.g., personnel screening)
13. A vulnerability management plan is developed and implemented

NIST CYBERSECURITY FRAMEWORK

- **PR. Maintenance**
- Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

NIST CYBERSECURITY FRAMEWORK

- **PR. Maintenance**

1. Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
2. Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

NIST CYBERSECURITY FRAMEWORK

- **PR. Protective Technology**
- Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements..

NIST CYBERSECURITY FRAMEWORK

- **PR. Protective Technology**

1. Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
2. Removable media is protected and its use restricted according to policy
3. The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
4. Communications and control networks are protected
5. Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations

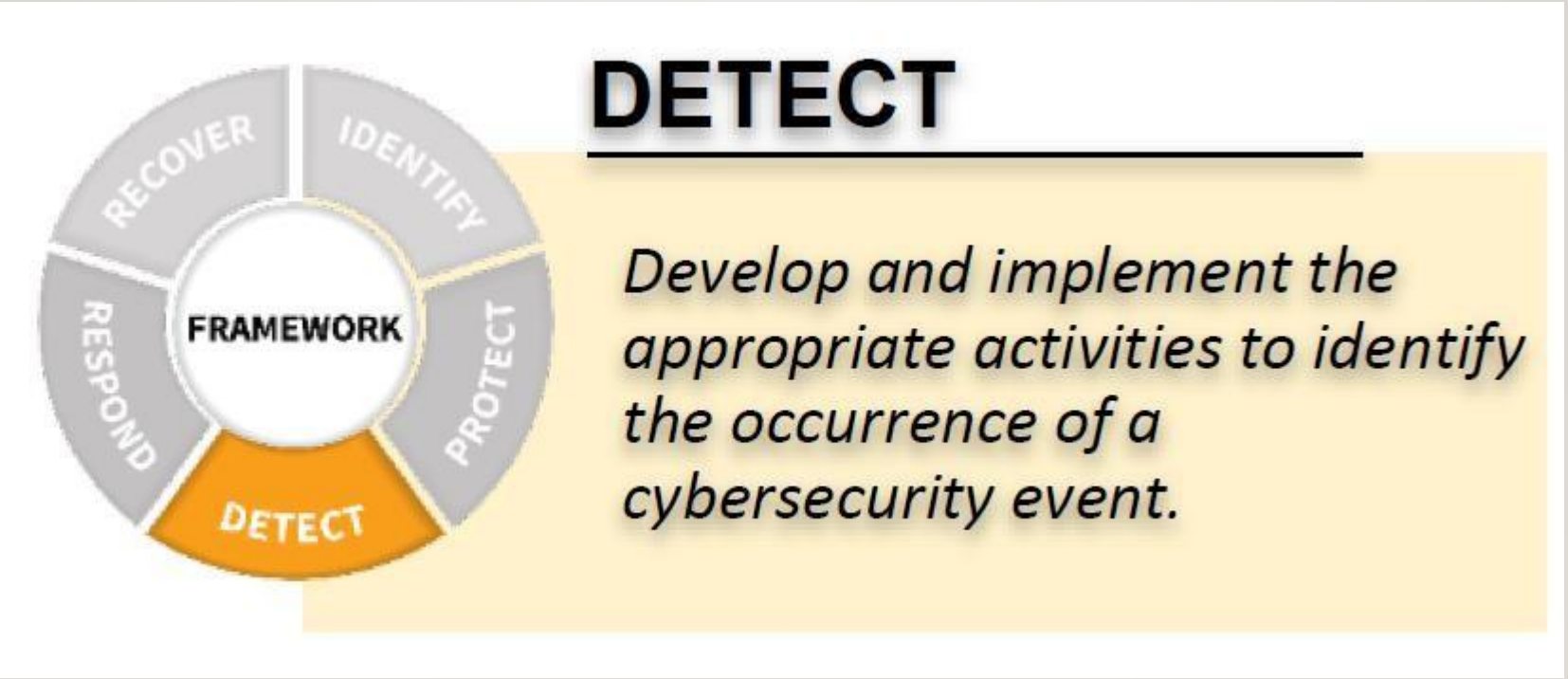
NIST CYBERSECURITY FRAMEWORK

- **PR. Protective Technology**

1. Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
2. Removable media is protected and its use restricted according to policy
3. The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
4. Communications and control networks are protected
5. Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations

NIST CYBERSECURITY FRAMEWORK

- **The Framework Core Structure :**
- **Detect(DE)**



NIST CYBERSECURITY FRAMEWORK

- **DE. Anomalies And Events**
- Anomalous activity is detected and the potential impact of events is understood.

NIST CYBERSECURITY FRAMEWORK

- **PR. Protective Technology**

1. A baseline of network operations and expected data flows for users and systems is established and managed
2. Detected events are analyzed to understand attack targets and methods
3. Event data are collected and correlated from multiple sources and sensors
4. Impact of events is determined
5. Incident alert thresholds are established

NIST CYBERSECURITY FRAMEWORK

- **DE. Security Continuous Monitoring**
- The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

NIST CYBERSECURITY FRAMEWORK

- **PR. Security Continuous Monitoring**

1. The network is monitored to detect potential cybersecurity events
2. The physical environment is monitored to detect potential cybersecurity events
3. Personnel activity is monitored to detect potential cybersecurity events
4. Malicious code is detected

NIST CYBERSECURITY FRAMEWORK

- **PR. Security Continuous Monitoring**

5. Unauthorized mobile code is detected
6. External service provider activity is monitored to detect potential cybersecurity events
7. Monitoring for unauthorized personnel, connections, devices, and software is performed
8. Vulnerability scans are performed

NIST CYBERSECURITY FRAMEWORK

- **DE. Detection Processes**
- Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

NIST CYBERSECURITY FRAMEWORK

- **DE. Detection Processes**

5. Roles and responsibilities for detection are well defined to ensure accountability
6. Detection activities comply with all applicable requirements
7. Detection processes are tested
8. Event detection information is communicated
9. Detection processes are continuously improved

NIST CYBERSECURITY FRAMEWORK

- **The Framework Core Structure :**
- **Respond(RS)**

NIST CYBERSECURITY FRAMEWORK

- **RS. Response Planning**
- Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. Response plan is executed during or after an incident

NIST CYBERSECURITY FRAMEWORK

- **RS**. **Communication**
- Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

NIST CYBERSECURITY FRAMEWORK

- **RS. Communication**

1. Personnel know their roles and order of operations when a response is needed
2. Incidents are reported consistent with established criteria
3. Information is shared consistent with response plans
4. Coordination with stakeholders occurs consistent with response plans
5. Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

NIST CYBERSECURITY FRAMEWORK

- **RS**. **Analysis**
- Analysis is conducted to ensure effective response and support recovery activities.

NIST CYBERSECURITY FRAMEWORK

- **RS**. **Analysis**

1. Notifications from detection systems are investigated
2. The impact of the incident is understood
3. Forensics are performed
4. Incidents are categorized consistent with response plans
5. Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).

NIST CYBERSECURITY FRAMEWORK

- **RS. Mitigation**
- Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

1. Incidents are contained
2. Incidents are mitigated
3. Newly identified vulnerabilities are mitigated or documented as accepted risks

NIST CYBERSECURITY FRAMEWORK

- **RS. Improvements**
- Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

1. Response plans incorporate lessons learned
2. Response strategies are updated

NIST CYBERSECURITY FRAMEWORK

- **The Framework Core Structure :**
- **Response(RC)**

NIST CYBERSECURITY FRAMEWORK

- **RC. Recovery Planning**
- Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents. Recovery plan is executed during or after a cybersecurity incident

NIST CYBERSECURITY FRAMEWORK

- **RE. Improvements**
- Recovery planning and processes are improved by incorporating lessons learned into future activities.

1. Recovery plans incorporate lessons learned
2. Recovery strategies are updated

NIST CYBERSECURITY FRAMEWORK

- **RE. Communications**

Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

NIST CYBERSECURITY FRAMEWORK

- **RE. Communications**

1. Public relations are managed
2. Reputation is repaired after an incident
3. Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

NIST CYBERSECURITY FRAMEWORK

- **Framework Profile**
- Alignment of cybersecurity functions, categories, and subcategories with organization's needs.
- **Current Profile**: Describes existing cybersecurity outcomes.
- **Target Profile**: Outlines desired outcomes for risk management goals.
- **Flexibility**: No preset templates, allowing customization.
- **Gap Analysis**: Identifies gaps between current and target profiles.
- **Risk-Based Approach**: Prioritizes actions based on organization's risk profile.

NIST CYBERSECURITY FRAMEWORK

- **Implementation Tiers Tiers:**
- To measure progress toward implementing the NIST Cybersecurity Framework, the framework identifies four implementation tiers:
- **Tier 1 – Partial:** Limited awareness and reactive approach to cybersecurity. Some controls implemented sporadically.
- **Tier 2 – Risk Informed:** Informal sharing of cybersecurity risks. Lack of formal, proactive risk management process.
- **Tier 3 – Repeatable:** Formalized risk management plan in place. Preparedness to monitor and respond to cyber threats.
- **Tier 4 – Adaptive:** Cyber resilient organization with continuous improvement. Integrated cybersecurity into organizational culture and budget decisions.

JORDAN NATIONAL CYBERSECURITY FRAMEWORK

- **JNCSF** is a comprehensive regulatory framework for public and private entities. This framework aims to combat cyber threats efficiently, enhancing technical, human, and administrative capabilities. By implementing policies, procedures, and controls, institutions bolster cybersecurity, positioning Jordan as a leader in the field. The overarching objective is to foster economic growth while bolstering institutional and human capacity to address cyber threats and minimize their impact on the kingdom.

JNCSF

- **Foundational Principles of the Regulatory Framework for Cybersecurity**
- **Organizational Capability:** Structuring institutions to implement cybersecurity strategies and enforce policies effectively.
- **Awareness and Training:** Increasing awareness of cyber threats and enhancing institutional capacity through employee training and educational resources.
- **Policy and Procedure Development:** Developing and improving cybersecurity policies and procedures, including risk management and incident handling.

JNCSF

- **Collaboration Enhancement:** Encouraging collaboration among institutions and stakeholders to enhance collective response capabilities to cyber threats.
- **Continuous Assessment and Review:** Implementing mechanisms for ongoing assessment and review of cybersecurity measures.

JNCSF

Jordan National Cybersecurity Framework Philosophy

1. Institutionalize Cybersecurity Risk Management across the Nation.

2.Transforming from COE as Center of Excellence to COE as Center of Enablement, where the National Cyber Security Center will develop programs to help Every Organization to become Cyber Security Center of Excellence.

3.Empower National Sector Regulators to Elevate the Sector Cyber Security Maturity Index

4. Cyber Security is Not a Technology Issue, Technology is

JNCSF

5. Promote the concept of Cyber Security Economics to help every organization develop a sophisticated, economically driven and cyber risk measurements that blends into their business plan.

6.Build the National Cyber Security Defender spirit in every Jordanian Citizen.

7. Build and Sustain National Capabilities through Academia.

8. Promote, direct and enable building National Cybersecurity Products

JNCSF

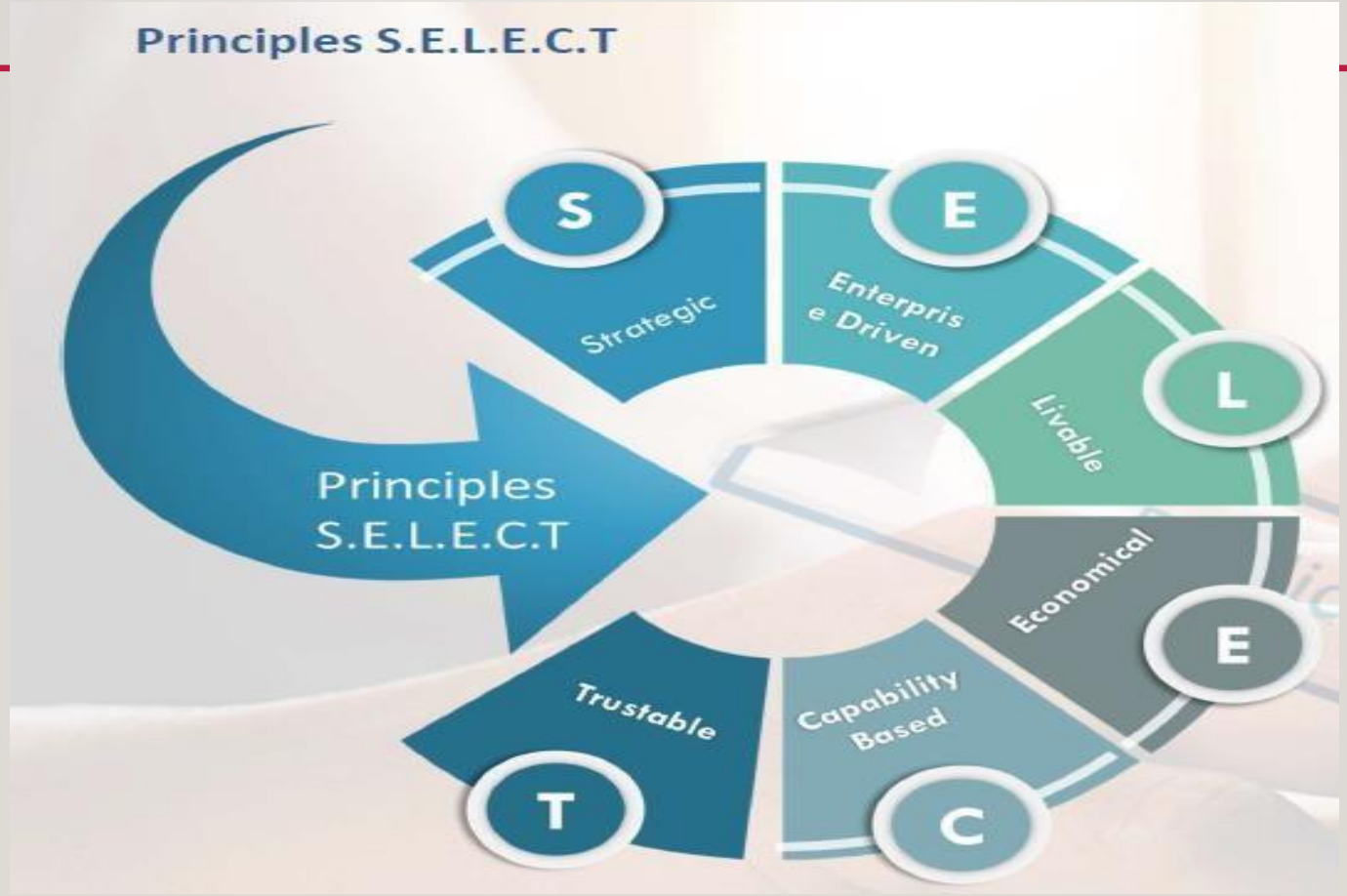
5. Promote the concept of Cyber Security Economics to help every organization develop a sophisticated, economically driven and cyber risk measurements that blends into their business plan.

6.Build the National Cyber Security Defender spirit in every Jordanian Citizen.

7. Build and Sustain National Capabilities through Academia.

8. Promote, direct and enable building National Cybersecurity Products

JNCSF


Principles S.E.L.E.C.T
Principles
S.E.L.E.C.T
S
Strategic
E
Enterpris
e Driven
L
Livable
E
Economical
C
Capability
Based
T
Trustable

JNCSF


Strategic
Cyber Security as Strategic Objective
National Concern, Every One is Responsible and Accountable
Protecting Data and Services
Business Problem Not Technology Problem
Protecting Data and Services
Information and Data are assets
Integrated in Digital Strategy
Protecting the Eco System

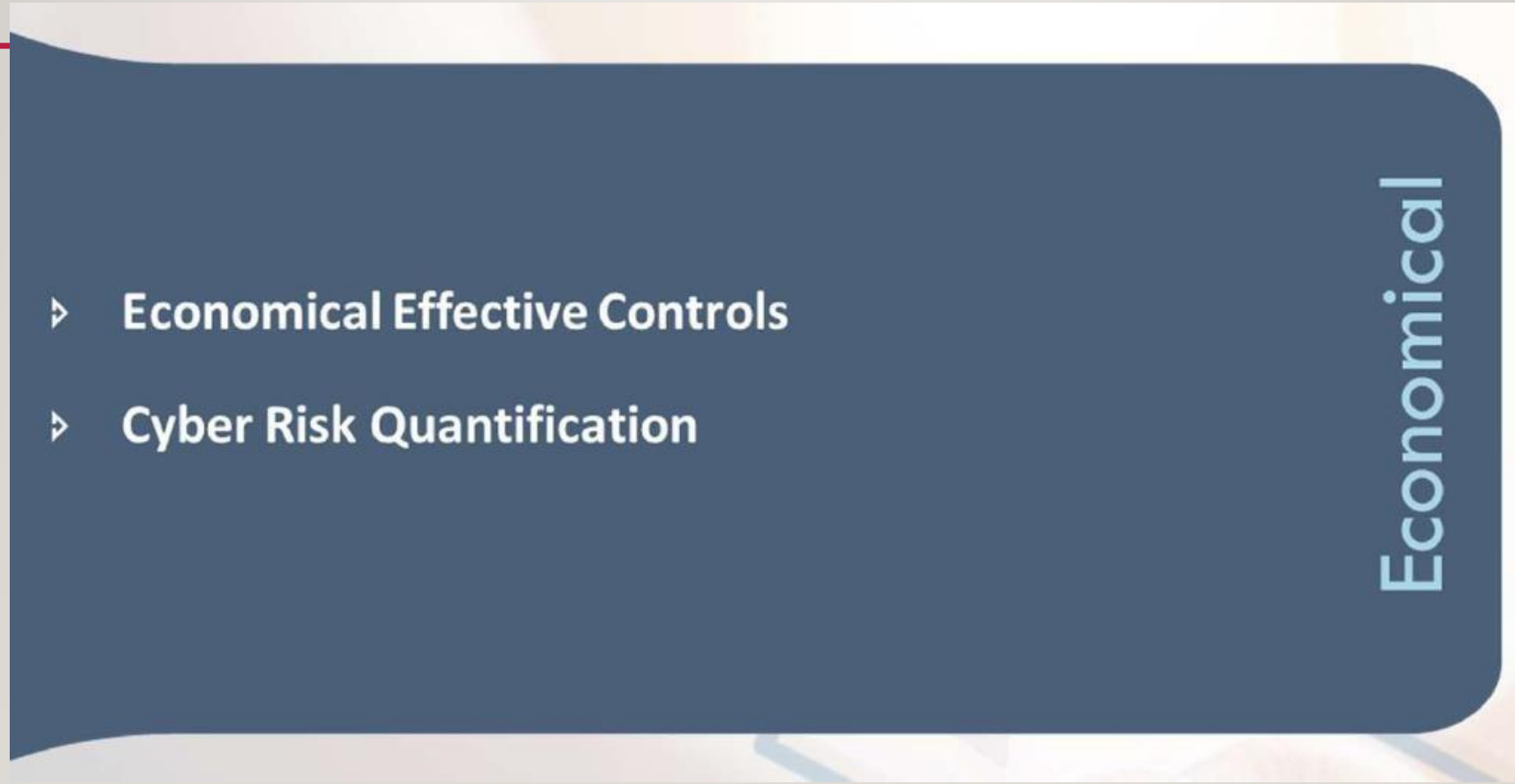
JNCSF


Cybersecurity Architecture
Organizational DNA Analysis
Security in Depth and Security by Design
Granular and Multi-Tier Risk Management Responsibilities
Cybersecurity Policies as Hierarchy
Enterprise Driven

JNCSF


Operational Cybersecurity Excellence
Systematic Continues Analysis
Continues Monitoring and live business dashboard
Livable

JNCSF


Economical Effective Controls
Cyber Risk Quantification
Economical

JNCSF


Organizational Capabilities
Sustainable National Skills and Qualifications
National Cybersecurity Products and Technologies
Capability Based

JNCSF


Trust is Vulnerability
Defensible Program
Risk based audit
Trustable

JNCSF

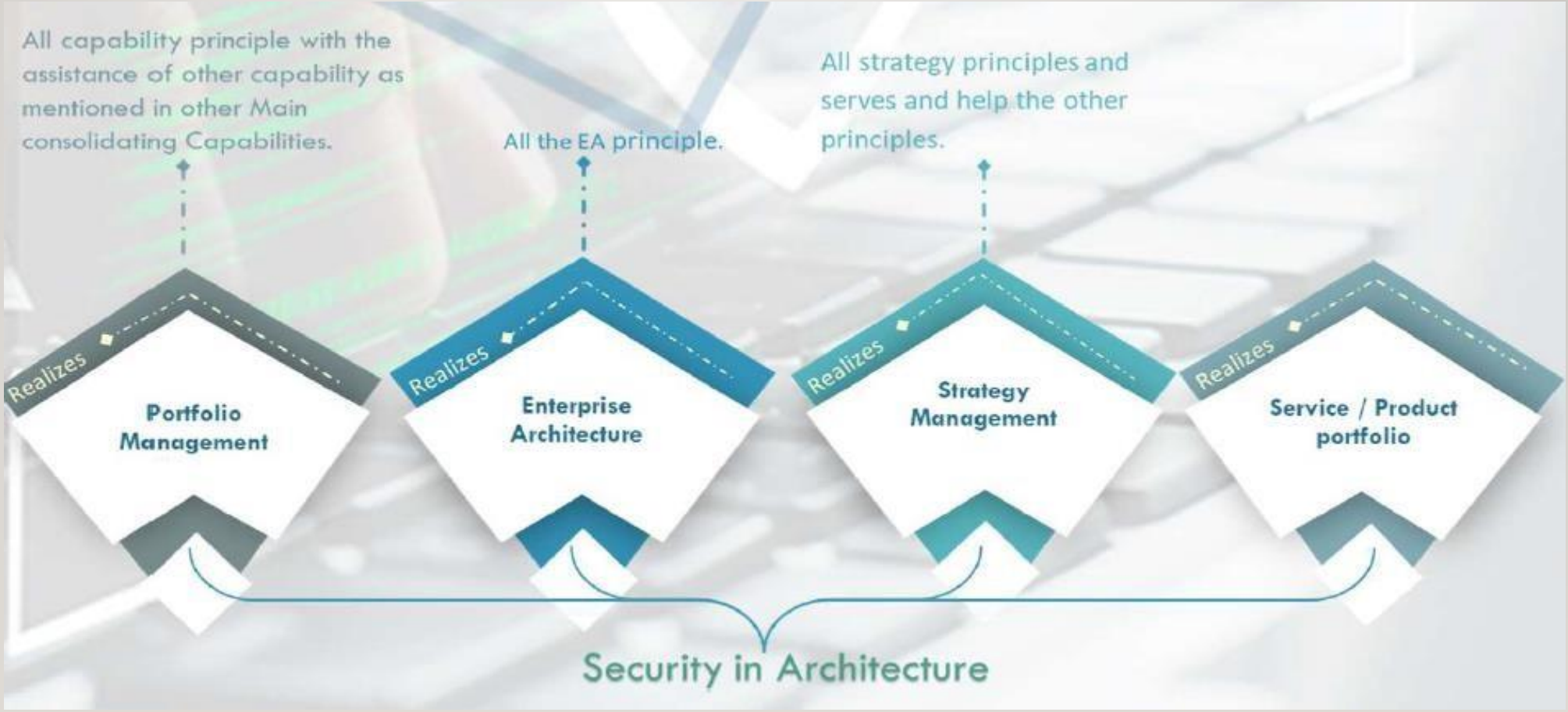
Jordan National Cybersecurity Framework Capabilities

JNCSF

JNCSF Capabilities

JNCSF

JNCSF Capabilities

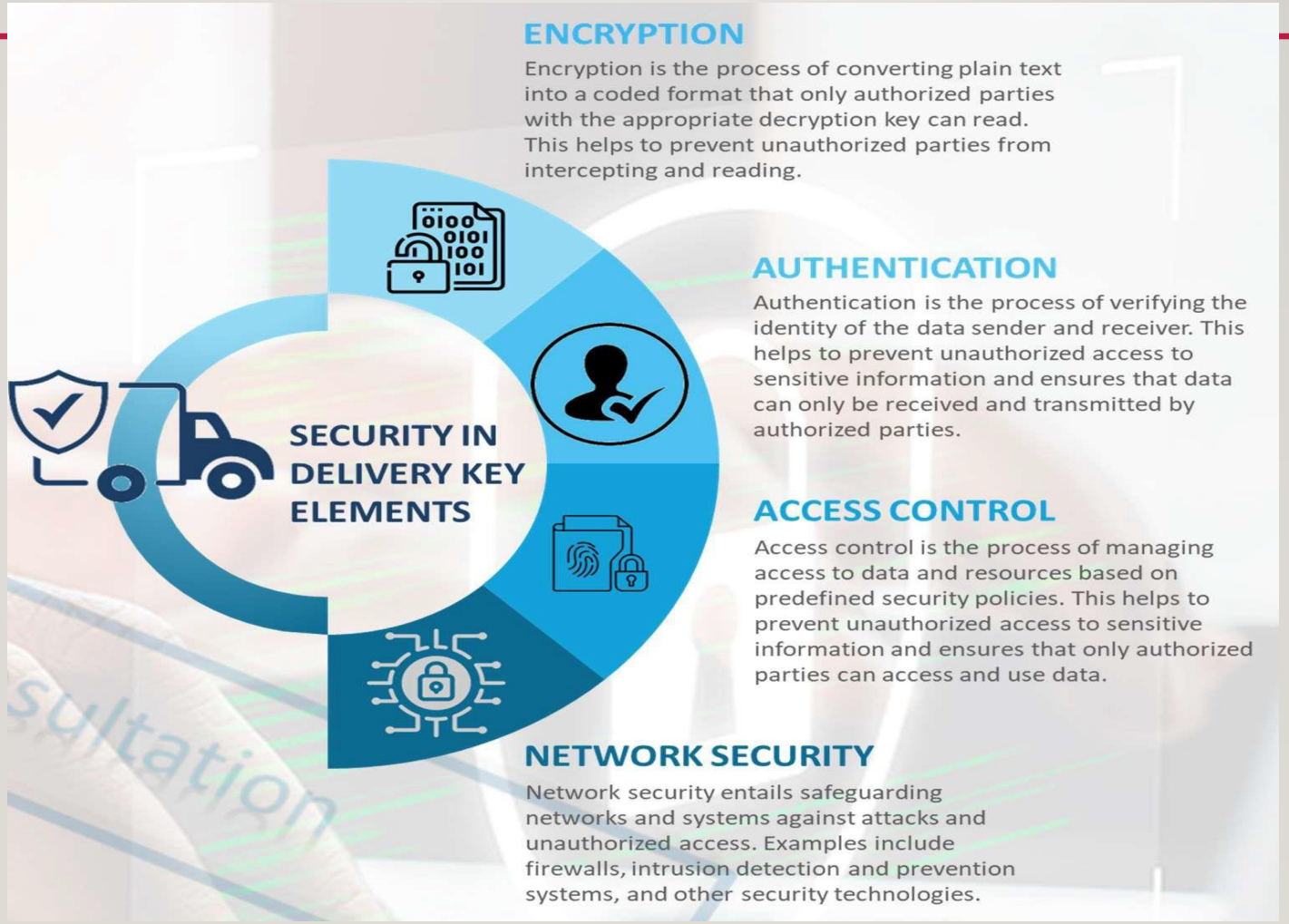


JNCSF

JNCSF Capabilities

JNCSF

JNCSF Capabilities



JNCSF

JNCSF Capabilities

JNCSF

JNCSF

Capabilities

JNCSF

JNCSF Capabilities

CYBERSECURITY REGULATIONS

- **Cybersecurity Regulations:** are governmental or industry-imposed standards dictating measures to protect digital systems, networks, and data from cyber threats. They encompass requirements for data encryption, access controls, incident response procedures, and risk assessments, aiming to ensure the confidentiality, integrity, and availability of information. Compliance is mandatory and failure to adhere can lead to legal consequences, financial penalties, and reputational harm.

JORDANIAN CYBERSECURITY LAW

- Cybersecurity Law :Law No. (16) of 2019
- Released on 16/9/2023.
- It consists of 19 articles.
- The main aim of the law is to protect information systems and networks from cybersecurity incidents, and the ability to restore and continue their work within a space that includes the interaction of people, data, information, information systems and their programs, communications systems and their associated infrastructure in an open global Cyber space.
- It is a regulatory law, not a legislative law.

PERSONAL DATA PROTECTION LAW.

- Personal Data Protection Law. :Law No. (24) of 2023
- Released on 17 /9/ 2023 and will be entered into force on 17/3/2024.
- It consists of 25 Articles.
- This legislation imposes several constraints on the handling of personal data, with a significant requirement being the necessity for explicit and documented consent, either in written or electronic form. Additionally, consent must be specific regarding duration and purpose, while citizens must be notified beforehand about the data collection's scope and reasons. Furthermore, the law prohibits processing data for any purposes other than those originally intended, with penalties for non-compliance.

NATIONAL CYBERSECURITY CENTER (NCSC)

- **Establishment :**
- With the increasing importance of cybersecurity, its threats, and issues related to it at the international level, and with the aim of protecting the Kingdom and its cyberspace, creating an umbrella that deals with cybersecurity issues has become a great importance and a pivotal role in preserving and promoting the interests of the country,

NATIONAL CYBERSECURITY CENTER (NCSC)

- **Establishment :**
- In addition to ensuring the safety of the work in various sectors at the country from any intrusions that may occur and with the tremendous development and the accompanying diversity in means of communication, computer programs and their applications, which has increased the volume and spread of information and data exchange, the National Center Cybersecurity for was established in accordance with Cybersecurity Law No. 16 of 2019.

NATIONAL CYBERSECURITY CENTER (NCSC)

- **Vision:**
- Jordanian cyberspace, Reliable and resistant to threats.

- **Mission:**
- Building, developing and organizing an effective cybersecurity system at the national level to protect the Kingdom from cyberspace threats and confront them efficiently and effectively in a way that ensures business sustainability, maintains national security, and enhances the confidence of national authorities, investors and individuals in Jordanian cyberspace.

NATIONAL CYBERSECURITY CENTER (NCSC)

- **Main Services:**
- Responding to cybersecurity incidents at the governmental and national levels, providing consultations and issuing reports related to them.
- Monitoring government networks, analyzing traffic records and data, for early detection of hacking cases that may be exposed to government systems, websites, and government institution networks, and notifying the concerned authorities.
- Analyze digital evidence, detect malware, and determine the cause and mechanism of the breach.

NATIONAL CYBERSECURITY CENTER (NCSC)

- Developing and implementing policies in the field of cybersecurity.
- Workshops on cybersecurity for various segments of society, including institutions and individuals.
- Training courses for individuals and institutions
- Information and cyber security competitions for school and university students.
- Security bulletins and advice for individuals about information security.

NATIONAL CYBERSECURITY CENTER (NCSC)

- Important bulletins and tips on security information.
- Granting licenses to cybersecurity service providers
- Receiving complaints and news related to cybersecurity incidents.
- Developing regulatory frameworks for governance and management of cybersecurity risks at the national level.

WHAT IS THE DIFFERENCE ?

What is the difference between NCSC and Anti-cyber crimes unit ?