

Cybersecurity in IoT

Part 2: Cybersecurity Domains

Agenda

1 Introduction

2 Domains Overview

a Security Strategy and Risk Management

b Security Governance

c Identity and Access Management

d Application Security

e Infrastructure Security

f Asset Security

g Cyber Defense

h Security Operations

3 NIST Security Domains

4 Case Study

5 Summary and Q&A

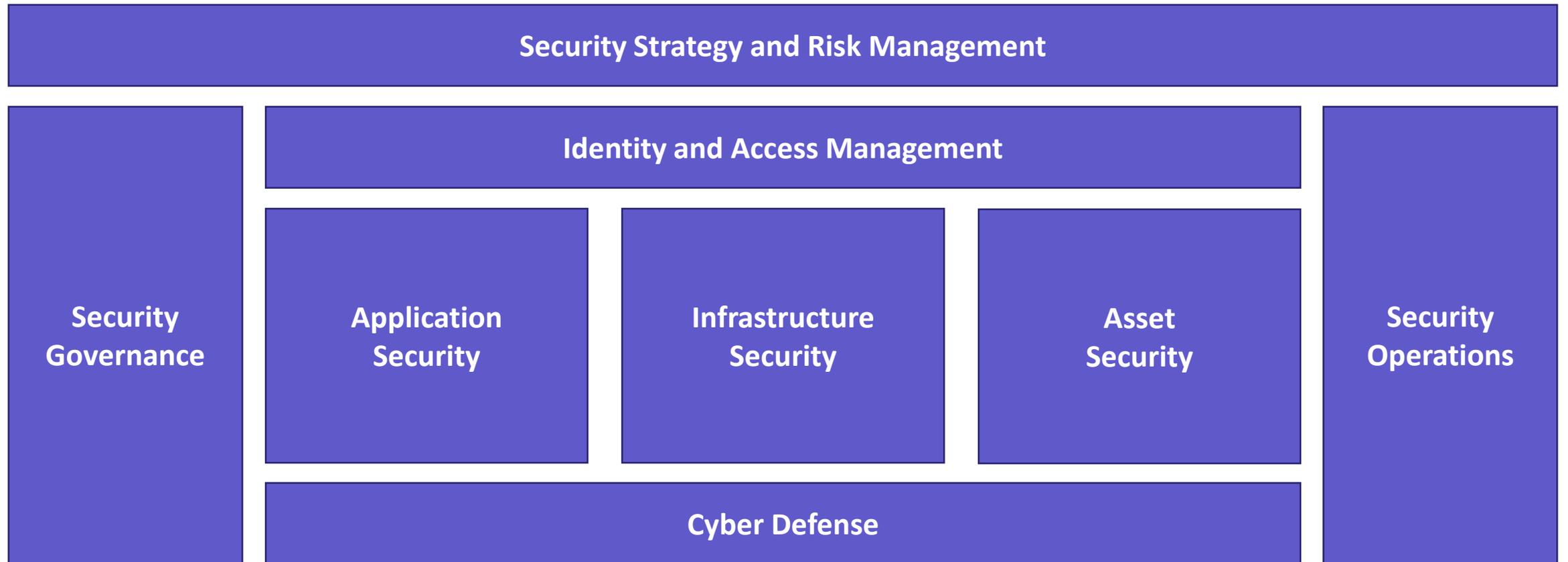
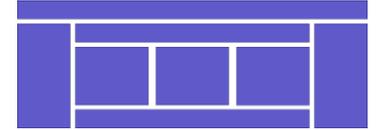
Cybersecurity Domains

Introduction

- Cybersecurity consists of a large diverse field of **different disciplines, technologies and processes**
- The domains introduced will give you a **high-level understanding** of what disciplines exist and how they are structured
- Two models will be introduced:
 - The first part is inspired by **CISSP** and the lecturers **personal experience**
 - The second provides a **NIST-based approach**
- *Note: There are many other valid ways to present the content of this chapter and there is **no clear cut** between the different disciplines, they often **overlap***

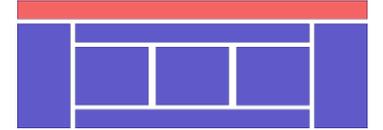


Cybersecurity Domains Overview

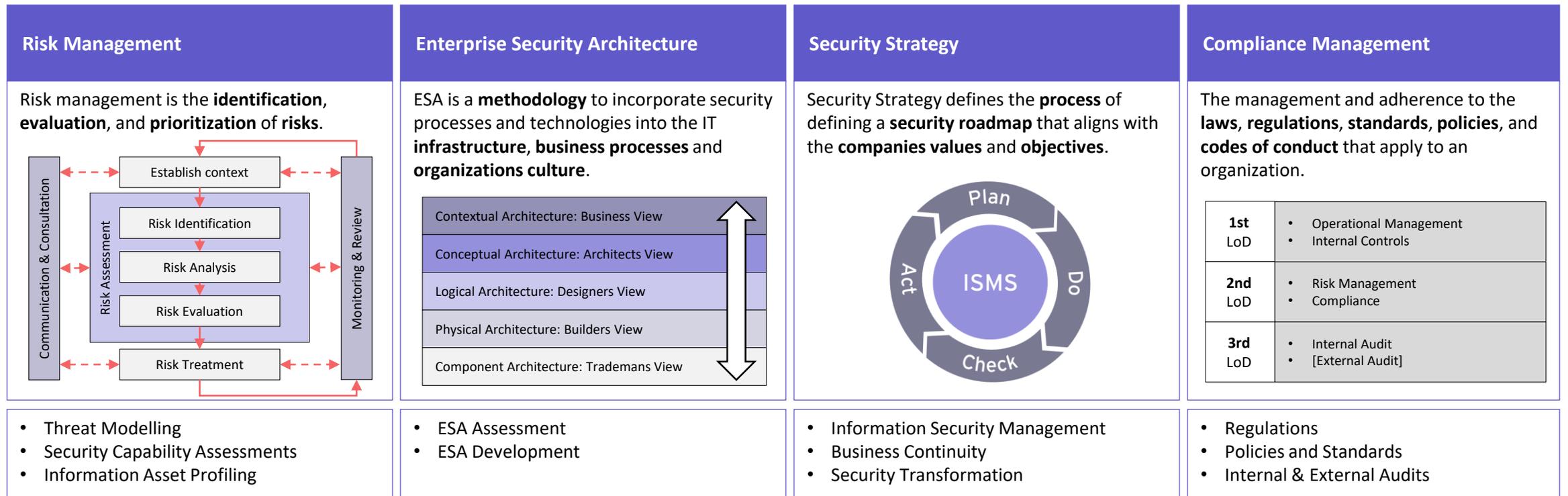


Cybersecurity Disciplines

Security Strategy and Risk Management

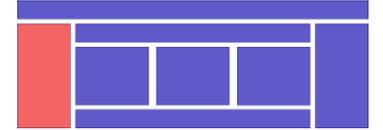


Defines roadmap to protect its **processes, assets and infrastructure** aligned to **business goals** and the organization's risk profile.



Cybersecurity Domains

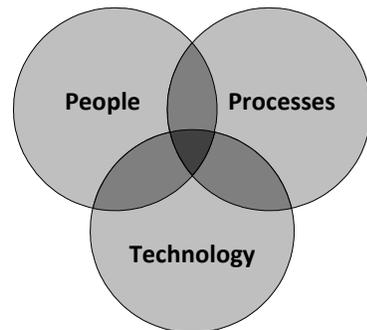
Security Governance



Establishing an **information security framework** aligned with the companies **goals, regulations and applicable laws**.

Security Program Management

The process of managing **people, processes** and **technologies** to implement the **security strategy** of the enterprise.



- Security Frameworks
- Security Processes
- Security Program Plan

Security Operating Model

A framework that **defines processes, responsibilities, oversight and governance** to enable effective security operations throughout the company.



- Security Control Framework
- Critical Security Functions
- Oversight and Management Controls

Security Awareness

One of the most important parts of cybersecurity. The **training and awareness** program serves to facilitate and **improve** the **security posture** of an organization.



- Secure workspace (e.g. clean-desk-policy)
- Security Awareness (e.g. Phishing)
- Training Security Personnel

Security Policy Management

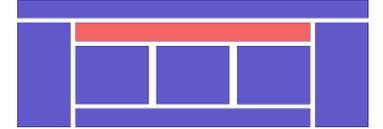
Responsible for **keeping** the **security policies updated and effective**. Further it needs to make sure that they are aligned with the company goals and communicated and enforced accordingly.



- Security Policy Program
- Security Policy Enforcement
- Security Policy Governance

Cybersecurity Domains

Identity and Access Management

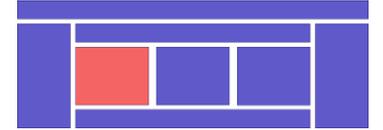


It defines and manages the **identities, roles** and **access privileges** of entities and individuals throughout the company.

Identity Management	Access Management	Authorization	Authentication
<p>The administrative process of assigning identities to users/devices and maintaining identities throughout their lifecycle.</p> 	<p>The process of assigning appropriate access permissions to identities.</p> 	<p>Authorization defines what a device or person is allowed to do. This can be based on roles or on an individual level.</p>  <p>Authorization What you can do</p>	<p>The mechanism to validate the identity of a given device or person.</p>  <p>Authentication Who you are</p>
<ul style="list-style-type: none"> • Provisioning • Account Management • Identity Life-cycle 	<ul style="list-style-type: none"> • Credential Management • Single Sign-On • Role Management 	<ul style="list-style-type: none"> • Role-based Access Control • Entitlement Management • Authorization policies 	<ul style="list-style-type: none"> • Biometric Authentication • Multi-Factor Authentication • Certificates

Cybersecurity Domains

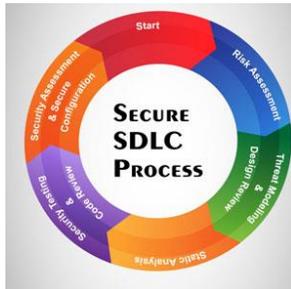
Application Security



Using **secure development practices** and improving security of an application by **fixing** and **preventing security vulnerabilities**.

Secure Development Lifecycle (SSDL)

The SSDL places security front and center during the application development process. From requirements to design, coding to test, it strives to build security into an application at every step in the development process.



- Application risk assessment
- Code review
- Secure development practices

Mobile and Web Application Security

The practice of safeguarding mobile and web applications from all forms of attacks. Due to the exposure of these applications operational security is key.



- Sandboxing
- Web application best practices
- Vulnerability scanning

Cloud Application Security

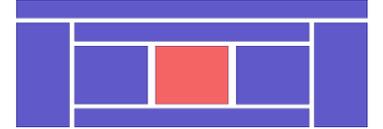
Protecting cloud applications comes with a new set of challenges and needs to be addressed accordingly. Many layers of the in-depth defense do not apply or are not in the control of the application owner.



- Cloud discovery
- Data leakage prevention
- Access control

Cybersecurity Domains

Infrastructure Security



Processes, policies and technologies that are focusing on the **protection** of **networks** and **devices** therein.

Endpoint Security

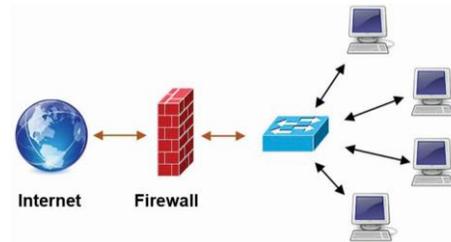
Endpoint security is a **methodology** for **protecting** a corporate or private network by focusing on **devices monitoring** their status, activities, software, authorization and authentication.



- Mobile device security
- Smart-device security
- Server security

Network Security

Network security describes the policies and procedures implemented to **avoid** and keep track of **unauthorized access, exploitation, modification**, or denial of the network and **network resources**.



- Perimeter security
- Wifi & area network security
- VPN

Platform Security

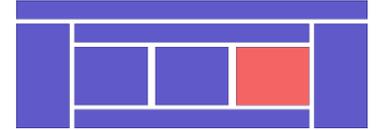
Platform security refers to the **security architecture**, tools and processes that ensure the **security** of an entire **computing platform**.



- Platform Security Architecture
- Trusted platform module
- IoT platform security

Cybersecurity Domains

Asset Security



Refers to the processes and technologies used to **protect information assets** and their **privacy** throughout their lifecycle.

Information Lifecycle (IL)

An Information Security Lifecycle describes the process of **securing information throughout** the different stages of its **lifecycle**



- Data storage
- The right to be forgotten
- Data retention

Data Loss and Leakage Prevention

Identify **sensitive information**, prevent accidental or malicious **loss of information**, **monitoring** data flows and **protecting** data.



- Personal Identifiable Information
- Regulations: GDPR / HIPAA
- Data monitoring

Data Protection

Data protection is the process of **safeguarding** important information from **corruption, compromise** or **loss**.



- Encryption
- Secure storage
- Access control

Data Privacy

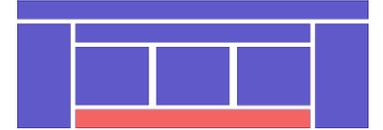
Information privacy is the privacy of **personal information** and relates to personal data, such as **medical records, financial data** or **criminal records**.



- Data Masking
- Tokenization
- Regulation and Compliance

Cybersecurity Domains

Cyber Defense



Managing **advanced threats (APT)** to the business by **gathering intelligence, detecting incidents** and **responding** accordingly.

Threat Intelligence

The process of gathering intelligence about threats and vulnerabilities. This data is then analyzed and filtered to produce threat intel feeds and management reports



- Threat gathering
- Threat analysis and modelling
- Vulnerability management

Threat Detection

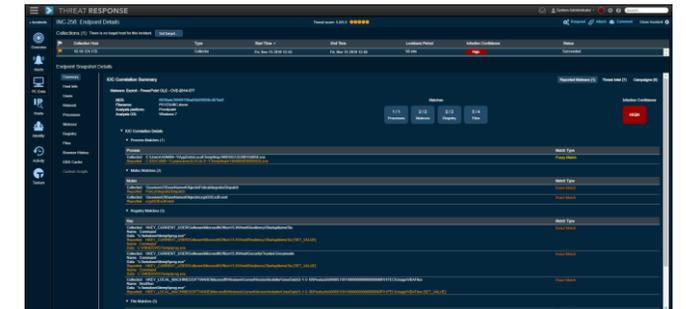
Threat detection is the process by which you find threats on your network, your systems or your applications. Identifying an attack early to minimize the impact.



- Security monitoring
- Security analytics
- Honeypots

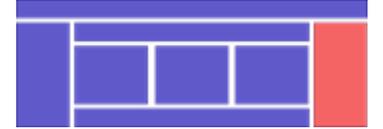
Threat Response

Threat response includes identifying, pursuing, and disrupting malicious cyber actors and activity, while reacting to the a possible attack and mitigating the impact.



- Incident triage
- Active Defense (Cyber threat hunting)
- Forensics

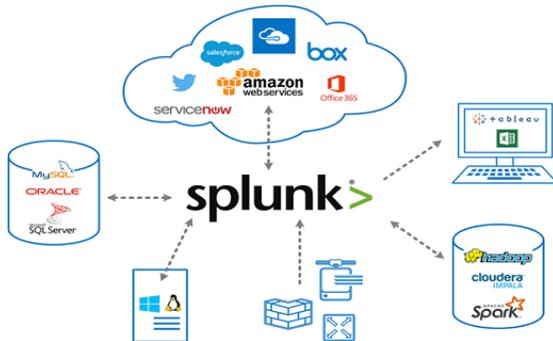
Cybersecurity Domains Security Operations



Concerned with the day-to-day activities of **detecting** and **protecting** sensitive and **business critical information**.

Security Incident and Event Management

SIEM as a blend of **real-time collection** and **analysis** of security **alerts** and correlation of events to deduce it to **detect incidents** and malicious patterns of behaviors.



- Security Operating Center
- Event and incident logging
- Incident dashboards

Patch and Upgrade Management

Patch and update management represents the process that involves the **acquisition, review, and deployment** of **patches** on an organization's systems.



- Patch auditing
- Patch testing
- Patch management tools

Compliance Monitoring

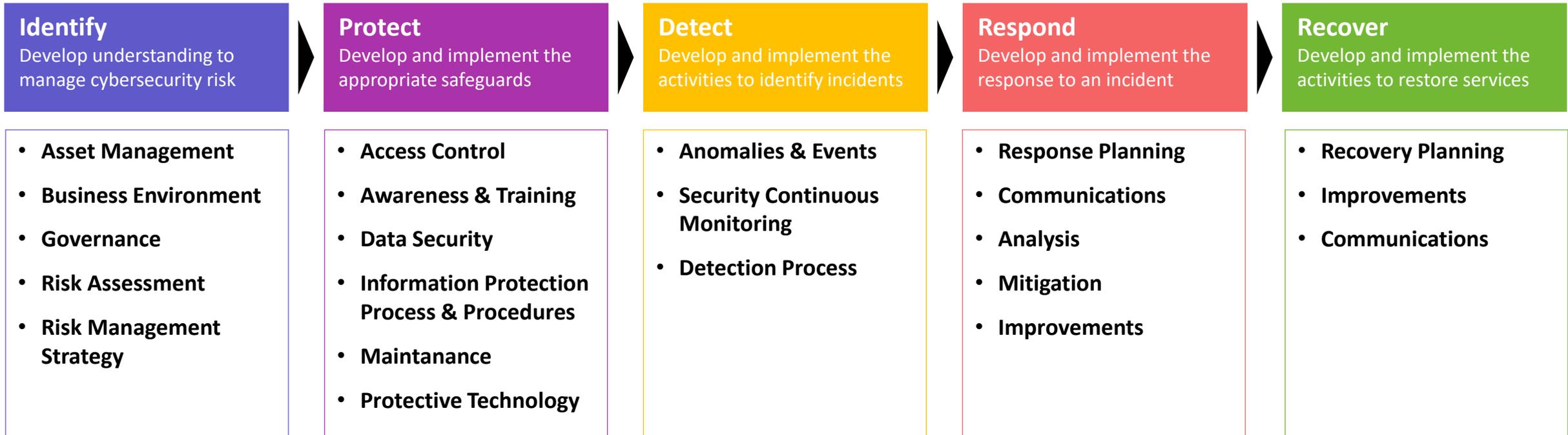
Compliance monitoring refers to the **quality assurance** tests organizations do, to check how well their **business operations** meet their **regulatory** and process **obligations**.



- Compliance monitoring plan
- Evidence archiving
- Internal audit

NIST Cybersecurity Framework

The NIST Cybersecurity Framework provides a **policy framework** of computer **security guidance** for how private sector organizations in the United States can assess and improve their ability to **prevent, detect, and respond** to cyber attacks.



Cybersecurity Foundation and Domains Summary

- **Fundamentals of Cybersecurity:**
 - Confidentiality, Integrity and **Availability**.
 - **Threat landscape:** Threat actor, threat, vulnerability, risk and countermeasures.
 - **Defense in-depth:** Many layers of security are required to secure information systems and assets.
 - **Administrative, technical** and **physical controls** need to be implemented to improve effectiveness.
- **Cybersecurity Domains:** High-level overview of cybersecurity disciplines, technologies and processes.
 - **Security Strategy and Risk Management** – Roadmap to protect its processes, assets and infrastructure.
 - **Security Governance** – An information security framework aligned with the companies goals, regulations and applicable laws.
 - **Identity and Access Management** – Defines and manages the identities, roles and access privileges of entities and individuals.
 - **Application Security** – Improving security of an application by fixing and preventing security vulnerabilities.
 - **Infrastructure Security** – Processes, policies and technologies that are focusing on the protection of networks and devices.
 - **Endpoint Security** – Processes and technologies used to protect information assets and their privacy throughout their lifecycle.
 - **Cyber Defense** – Managing threats to the business by gathering intelligence, detecting incidents and responding accordingly.
 - **Security Operations** – day-to-day activities of detecting and protecting sensitive and business critical information.
- **NIST Cybersecurity Framework:** Policy framework of computer security guidance (Identify, Protect, Detect, Respond, Recover)



Thank you!

