# OTHM Level-4 Diploma

## Diploma in Information and Technology

## Cyber Security

## Lesson Two

**U Tin Naing Htwe**
**Senior Lecturer(ICT)**
**Optimum Institute**

# Today's Lesson

## Cyber Security

# Cyber Security


1. Understand the fundamentals of cyber security.
2. Understand cyber security protection methods.
3. Understand how to manage a cyber security attack.

# 1. “ Understand the fundamentals of cyber security ”

1.1 Define the term ‘cyber security’.

1.2 Explain how cyber security risks are managed in an organisation.

1.3 Describe the laws and regulations associated with cyber security

1.4 Summarise the historical development of cyber security.

1.5 Explain the impact cyber security has on individuals and organisations.

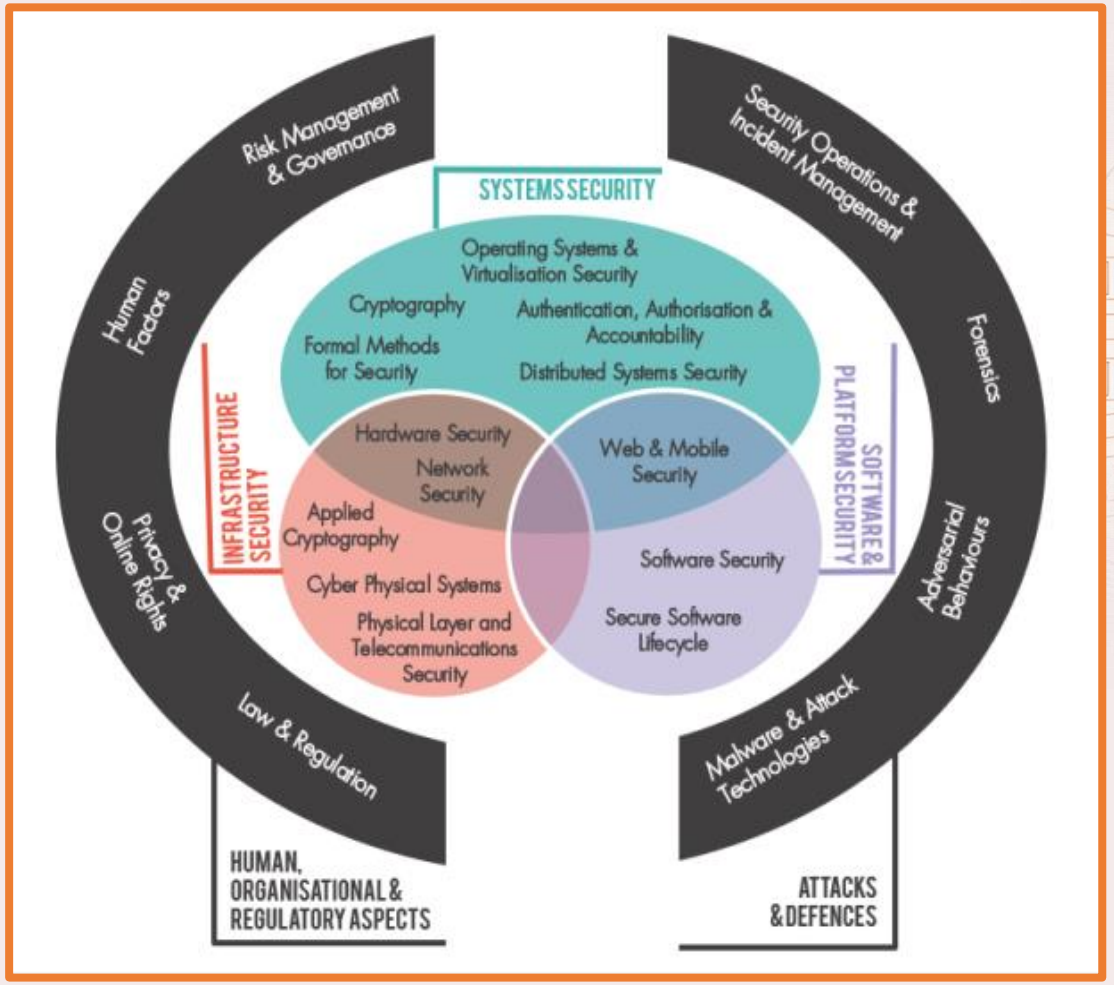
1.6 Explain how to keep up to date with the latest cyber security information.

# Part 1

## 1.2 Explain how cyber security risks are managed in an organization.

# The 21 Knowledge Areas (KAs) in the CyBOK Scope

# Cyber Security Body Of Knowledge (CyBOK)




1. Human Organisational and Regulatory Aspects
2. Attacks and Defences
3. System Security
4. Software Platform Security
5. Infrastructure Security

**4 + 4 + 5 + 3 + 5 = 21 Knowledge (CyBOK)**

Risk Management & Governance

Law & Regulation

Human Factors

Privacy & Online Rights

Malware & Attack Technologies

Adversarial Behaviours

Security Operations & Incident Management

Forensics

Cryptography

Operating Systems & Virtualisation Security

Distributed Systems Security

Formal Methods for Security

Authentication, Authorisation & Accountability

Software Security

Web & Mobile Security

Secure Software Lifecycle

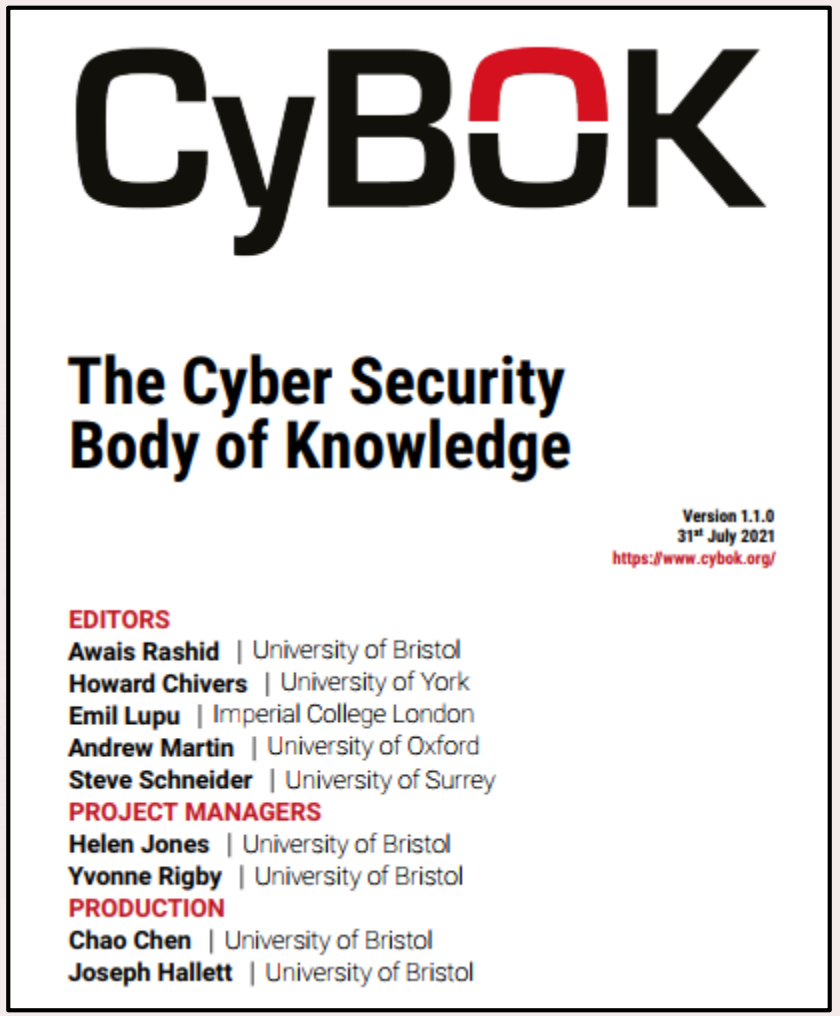
Applied Cryptography

Network Security

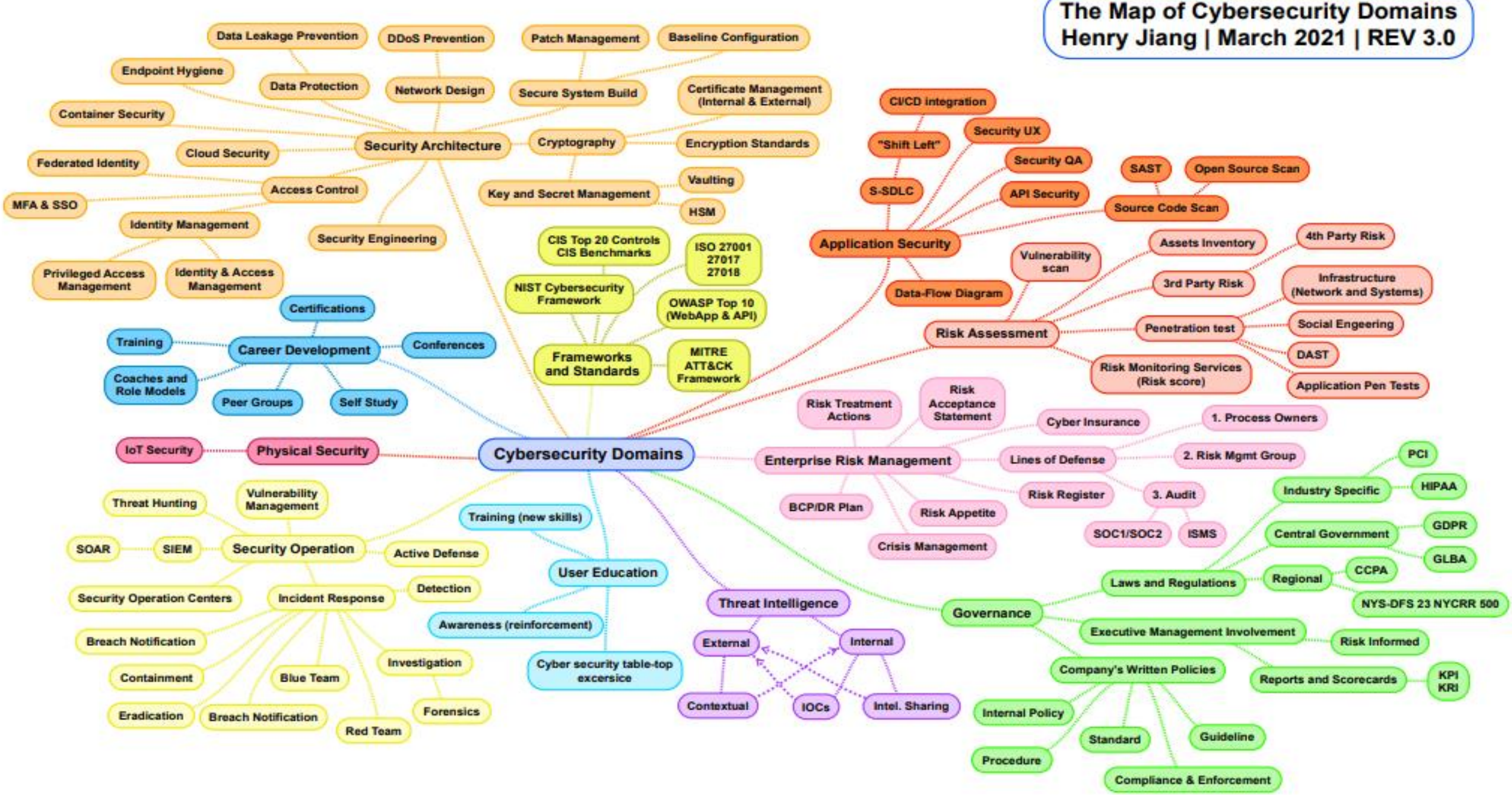
Hardware Security

Cyber-Physical Systems Security

Physical Layer & Telecommunications Security




**4 + 4 + 5 + 3 + 5 = 21 Knowledge (CyBOK)**

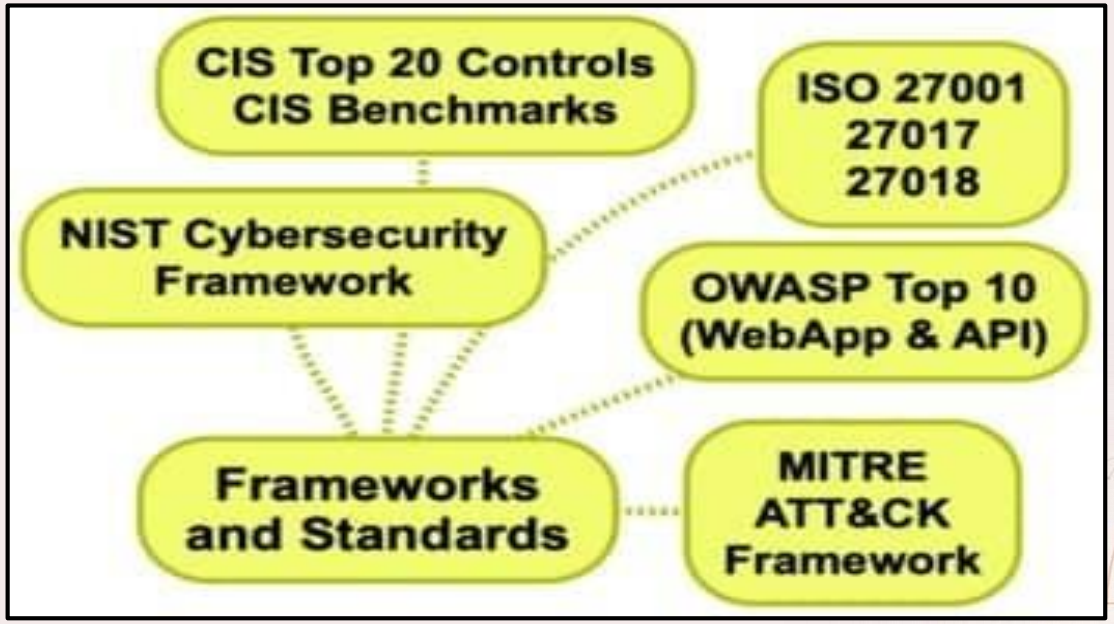

The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.0
Cybersecurity Domains
Security Architecture
Data Leakage Prevention
DDoS Prevention
Patch Management
Baseline Configuration
Endpoint Hygiene
Data Protection
Network Design
Secure System Build
Certificate Management (Internal & External)
Container Security
Cryptography
Encryption Standards
Cloud Security
Federated Identity
Access Control
Key and Secret Management
Vaulting
HSM
MFA & SSO
Identity Management
Security Engineering
Privileged Access Management
Identity & Access Management
Application Security
CI/CD integration
"Shift Left"
Security UX
Security QA
S-SDLC
API Security
SAST
Open Source Scan
Source Code Scan
Data-Flow Diagram
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Infrastructure (Network and Systems)
Risk Assessment
Penetration test
Social Engeering
DAST
Risk Monitoring Services (Risk score)
Application Pen Tests
Frameworks and Standards
CIS Top 20 Controls
CIS Benchmarks
ISO 27001
27017
27018
NIST Cybersecurity Framework
OWASP Top 10 (WebApp & API)
MITRE ATT&CK Framework
Career Development
Certifications
Training
Conferences
Coaches and Role Models
Peer Groups
Self Study
Physical Security
IoT Security
Enterprise Risk Management
Risk Treatment Actions
Risk Acceptance Statement
Cyber Insurance
1. Process Owners
Lines of Defense
2. Risk Mgmt Group
Risk Register
3. Audit
BCP/DR Plan
Risk Appetite
SOC1/SOC2
ISMS
Crisis Management
Security Operation
Threat Hunting
Vulnerability Management
SOAR
SIEM
Active Defense
Security Operation Centers
Incident Response
Detection
Breach Notification
Containment
Blue Team
Investigation
Eradication
Breach Notification
Forensics
Red Team
User Education
Training (new skills)
Awareness (reinforcement)
Cyber security table-top excersice
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
Governance
Laws and Regulations
Industry Specific
PCI
HIPAA
Central Government
GDPR
GLBA
Regional
CCPA
NYS-DFS 23 NYCRR 500
Executive Management Involvement
Risk Informed
Company's Written Policies
Reports and Scorecards
KPI
KRI
Internal Policy
Standard
Guideline
Procedure
Compliance & Enforcement

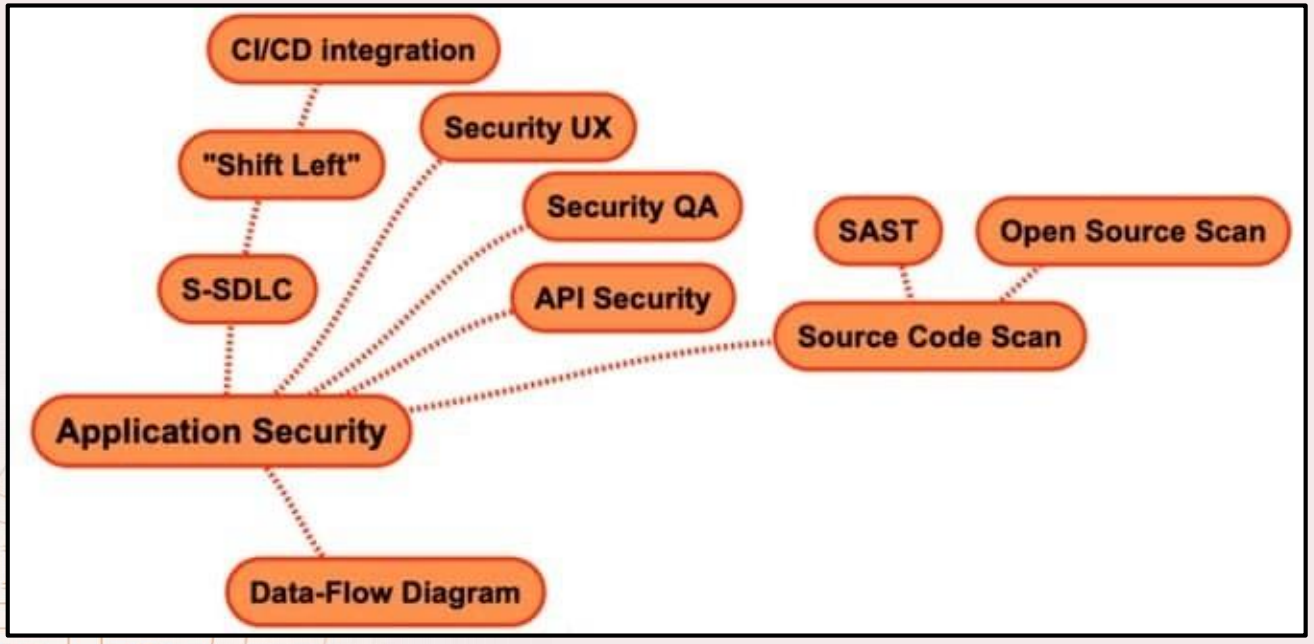
# 11 Domains Knowledge of Cyber Security

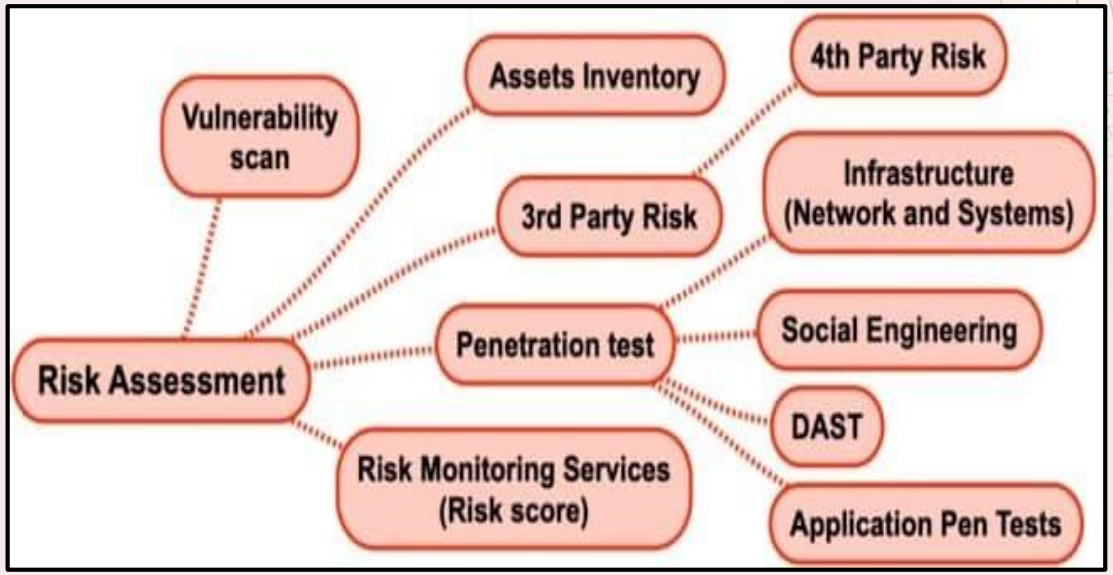
1. Frameworks and Standards
2. Application Security
3. Risk Assessment
4. Enterprise Risk Management
5. Governance
6. Threat Intelligence
7. User Education
8. Security Operations
9. Physical Security
10. Career Development
11. Security Architecture

**Certified Information Systems Security Professional**


https://myturn.careers/blog/cyber-security-domains-do-they-exist/

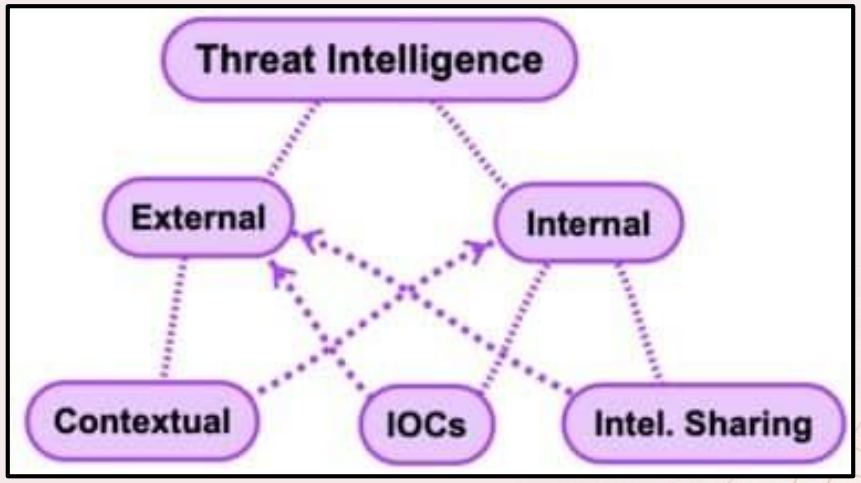

CIS Top 20 Controls
CIS Benchmarks
ISO 27001
27017
27018
NIST Cybersecurity Framework
OWASP Top 10 (WebApp & API)
Frameworks and Standards
MITRE ATT&CK Framework

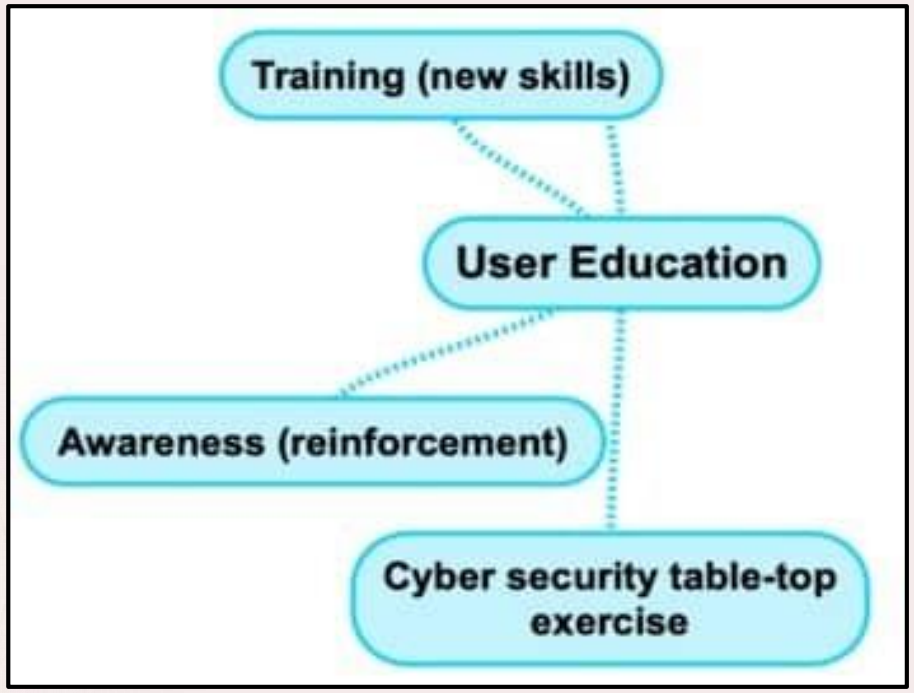

CI/CD integration
Security UX
"Shift Left"
Security QA
SAST
Open Source Scan
S-SDLC
API Security
Source Code Scan
Application Security
Data-Flow Diagram


Assets Inventory
4th Party Risk
Vulnerability scan
Infrastructure (Network and Systems)
3rd Party Risk
Penetration test
Social Engineering
Risk Assessment
DAST
Risk Monitoring Services (Risk score)
Application Pen Tests

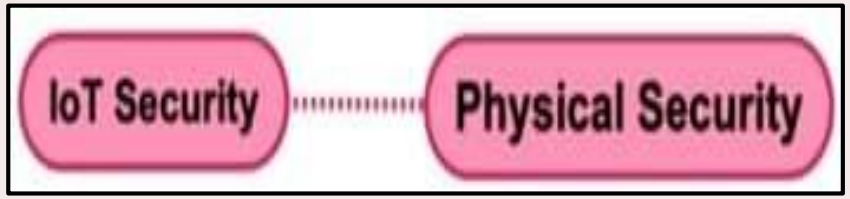

Risk Acceptance Statement
Risk Treatment Actions
Cyber Insurance
1. Process Owners
Enterprise Risk Management
Lines of Defense
2. Risk Mgmt Group
Risk Register
3. Audit
BCP/DR
Risk Appetite
SOC1/SOC2
Crisis Management


PCI
Industry Specific
HIPAA
Central Government
GDPR
GLBA
Laws and Regulations
Regional
CCPA
Governance
NYS-DFS 23 NYCRR 500
Executive Management Involvement
Risk Informed
Reports and Scorecards
KPIs/KRIs
Policy
Company's Written Policies
Procedure
Standard
Guideline
Compliance & Enforcement

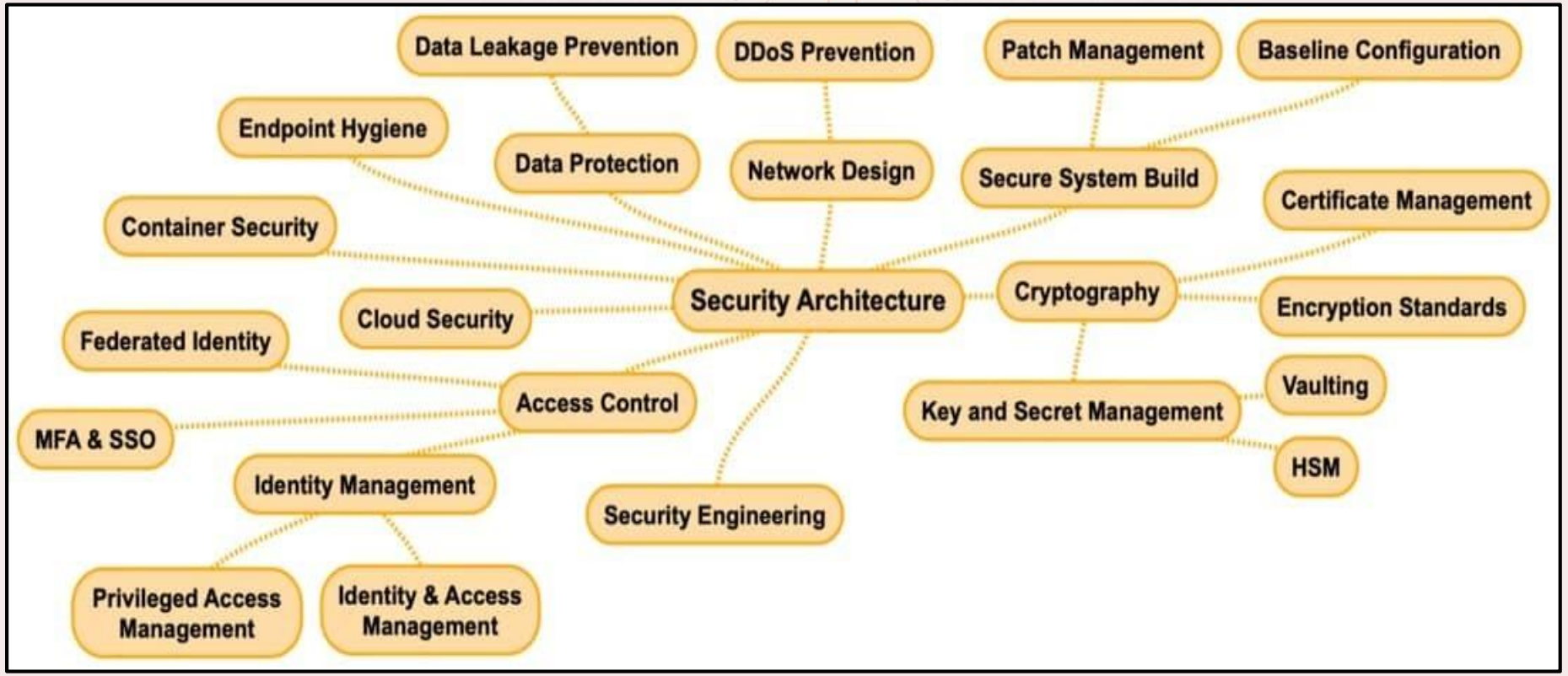

Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing


Training (new skills)
User Education
Awareness (reinforcement)
Cyber security table-top exercise


Threat Hunting
Vulnerability Management
SOAR
SIEM
Security Operation
Active Defense
Security Operation Centers
Incident Response
Detection
Breach Notification
Investigation
Containment
Blue Team
Red Team
Forensics
Eradication


IoT Security
Physical Security


Certifications
Training
Career Development
Conferences
Coaches and Role Models
Peer Groups
Self Study


Data Leakage Prevention
DDoS Prevention
Patch Management
Baseline Configuration
Endpoint Hygiene
Data Protection
Network Design
Secure System Build
Certificate Management
Container Security
Security Architecture
Cryptography
Encryption Standards
Cloud Security
Federated Identity
Access Control
Vaulting
Key and Secret Management
MFA & SSO
HSM
Identity Management
Security Engineering
Privileged Access Management
Identity & Access Management

# How does cyber security work?

Cybersecurity uses **people, processes and technology** to protect businesses from cyber threats.

**People** with highly specialized skills provide round-the-clock eyes on the business digital environment to safe guard them from potential cyber threats and attacks.

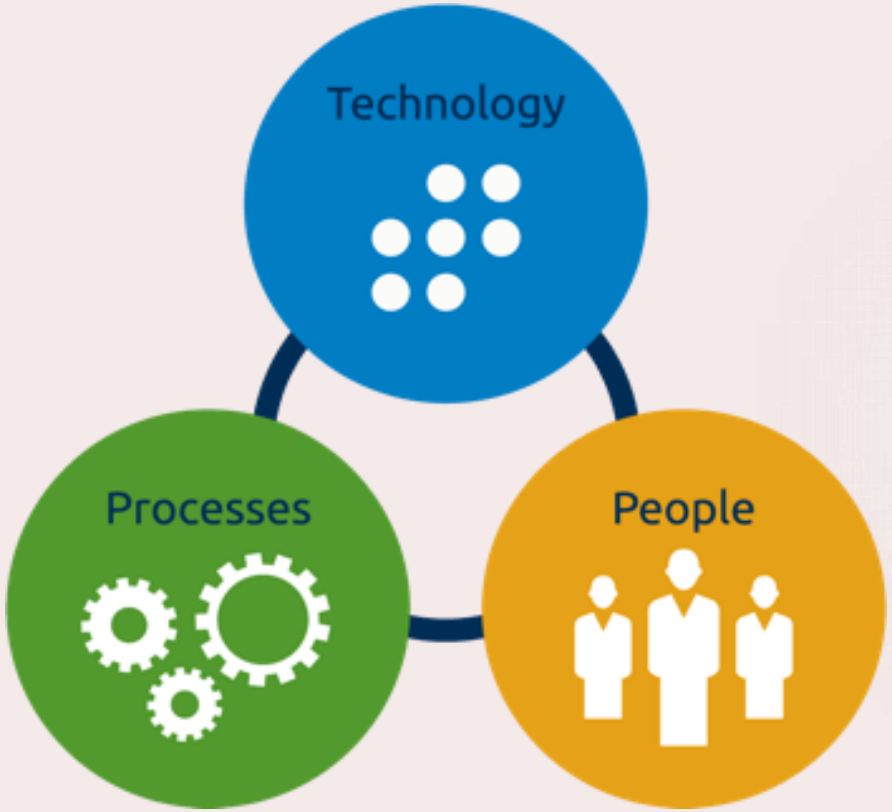
- ✓ *These heroes are know by the following names; Managed Security Services, Cyber Security Analysts, Threat Hunter, Blue Team, Red Team, Purple teams, Ethical Hackers/Penetration Testers and more*.

**Processes** include **Security Operation Centers (SOC)**, security compliance to industry standards, and security audits. A SOC runs **24x7x365** on digital assets in a business using many processes for monitoring, detecting and neutralizing cyber threats and attacks.

- ✓ *A business may choose to comply with guidelines from security frameworks such as NIST and ISO27000. Regular security audits can be performed by businesses to insure that their security policy is being followed. All of these put together constitute the processes needed by a business to secure itself*.

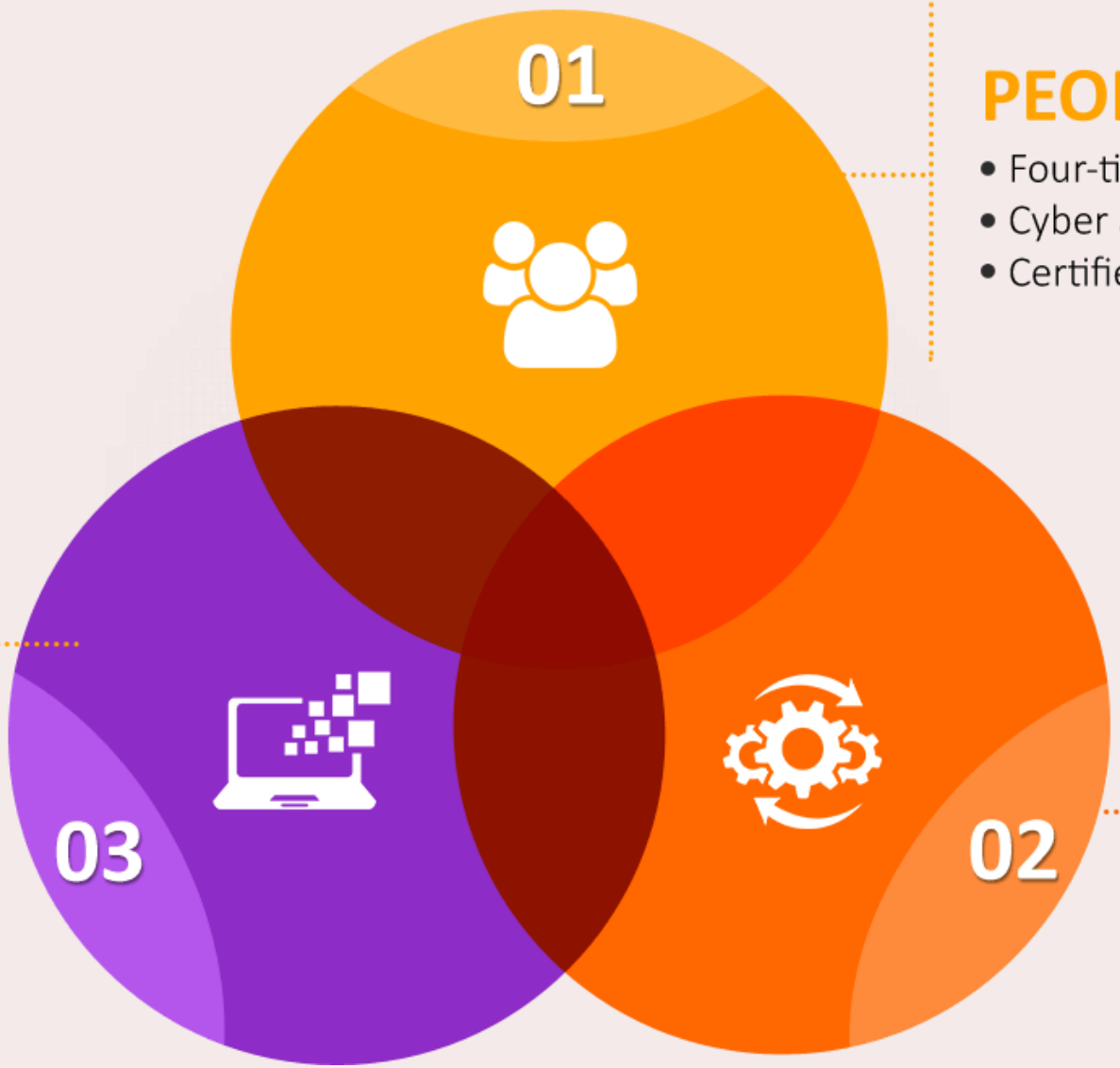
**Technology** is the brawn of the cyber security world and do the heavy lifting of examining millions of threats from various threat vectors.

- ✓ *They use state of the art technologies such as Artificial Intelligence, Machine Learning, synchronized security, next-gen security for endpoints, Wi-Fi, network, mobile devices and SOAR (Security Orchestration, Automation and Response) platforms*.




**SOC team performs the following functions:**

1. Active monitoring and analysis of all integrated systems
2. Detection of IT vulnerabilities
3. Checking Compliance
4. Central management of all integrated devices
5. Notifies you about attacks and threats
6. Defensive measures to limit damage
7. Security Assessments
8. Detailed reporting




## PEOPLE

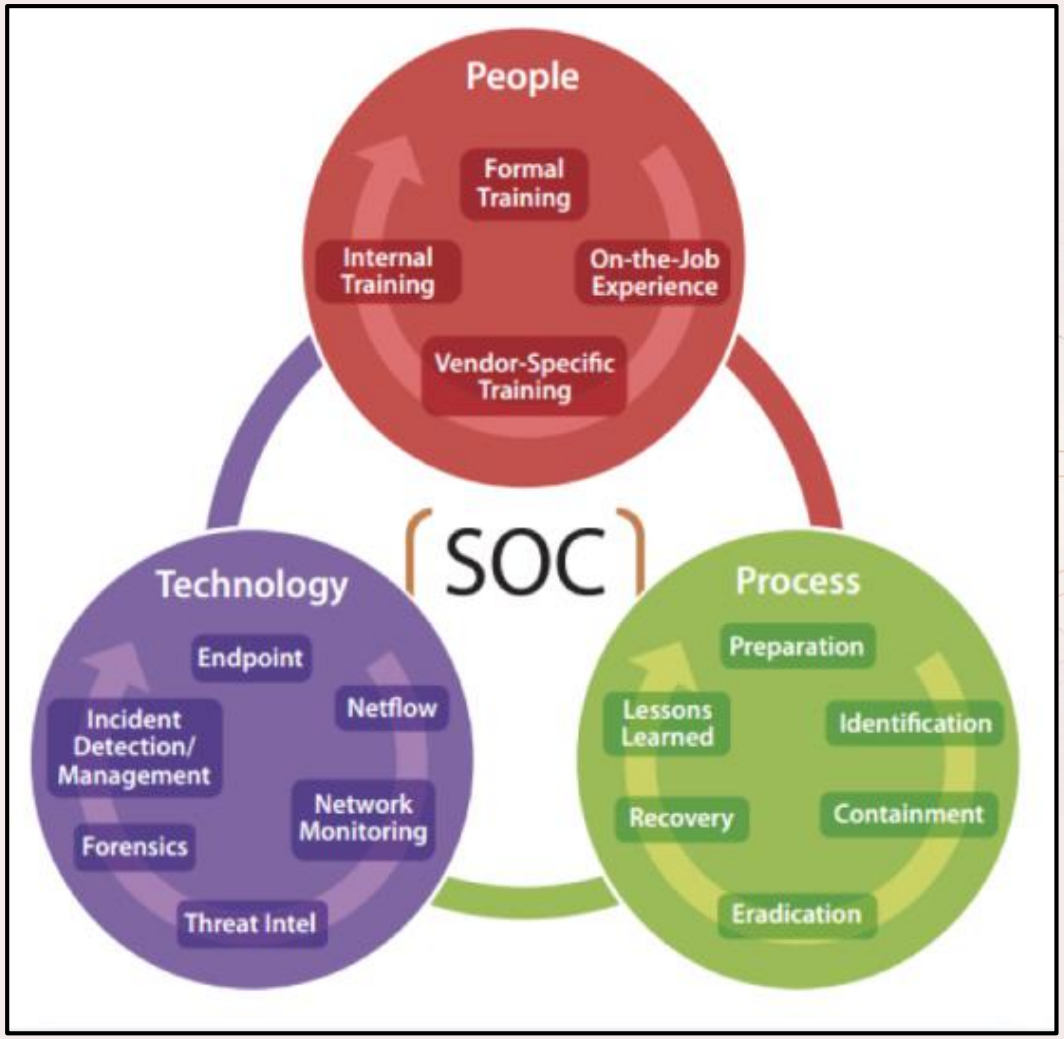
- Four-tier SOC team
- Cyber architectural engineers
- Certified risk professionals

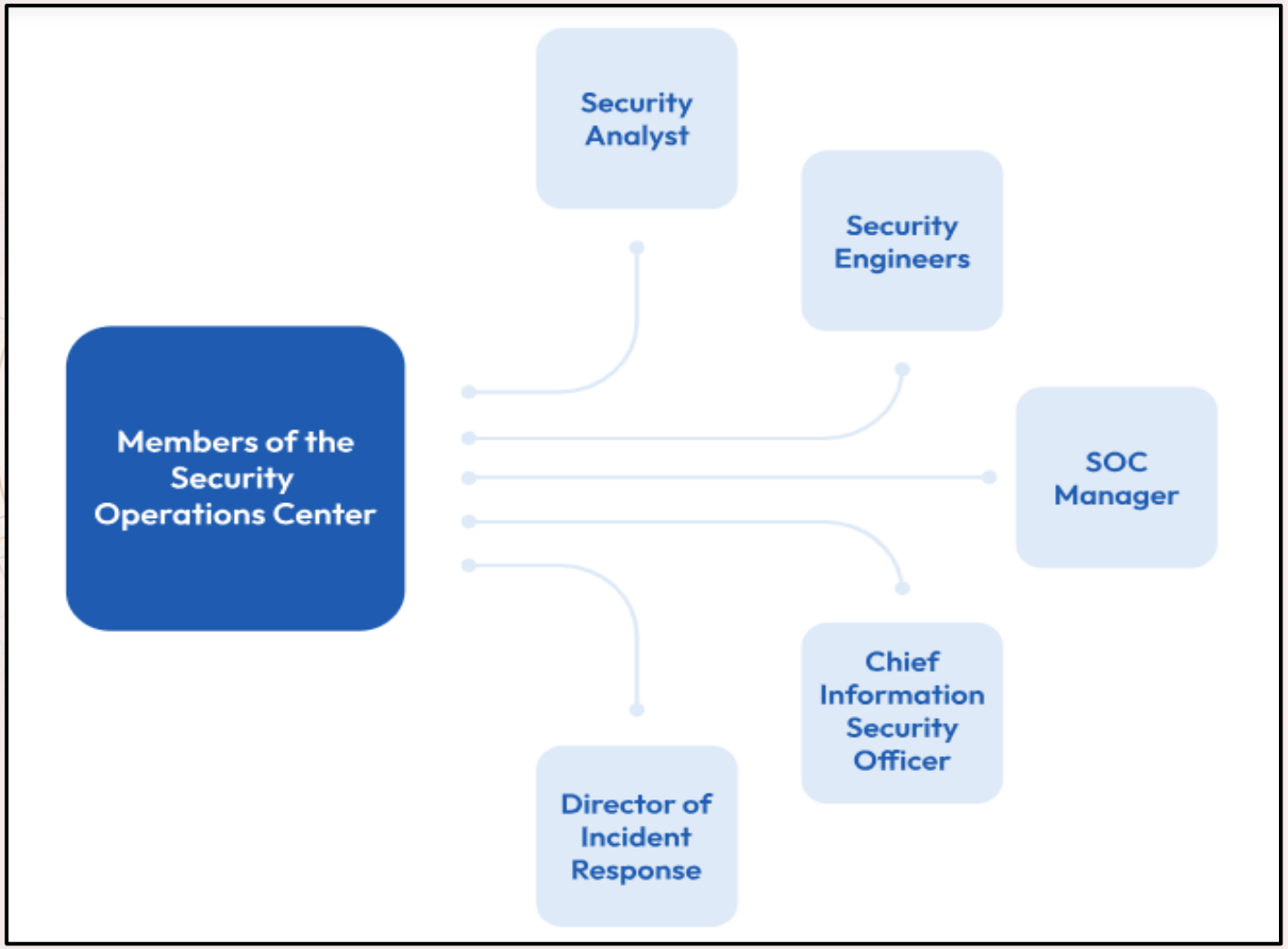
## PROCESS

- SOC Orchestration
- Threat detection
- Vulnerability scanning
- Network threat analytics

## TECHNOLOGY

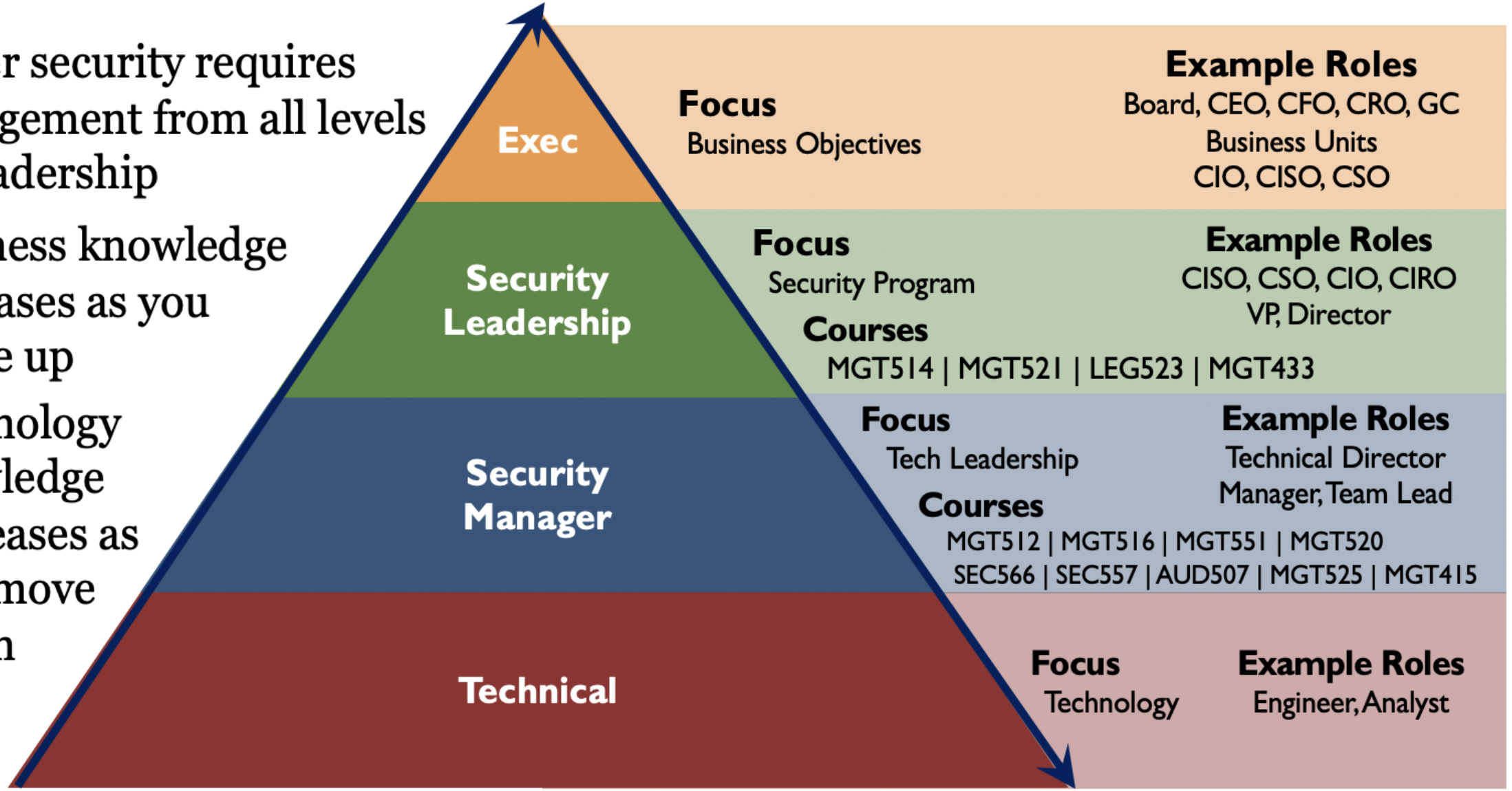
- Alert and reporting
- Alarms and escalation
- Defined use cases
- Automated ticketing
- Incident breach response
- Reporting and dashboards


People
Formal Training
Internal Training
On-the-Job Experience
Vendor-Specific Training
SOC
Technology
Endpoint
Netflow
Incident Detection/ Management
Network Monitoring
Forensics
Threat Intel
Process
Preparation
Lessons Learned
Identification
Recovery
Containment
Eradication


Members of the Security Operations Center
Security Analyst
Security Engineers
SOC Manager
Chief Information Security Officer
Director of Incident Response

# Cyber Leadership

- Cyber security requires engagement from all levels of leadership
- Business knowledge increases as you move up
- Technology knowledge increases as you move down



# Layout of Security Operations Center (SOC)

# What is cyber security risk management?

- Cyber risk management means **identifying**, **analysing**, **evaluating** and **addressing** your organisation's cyber security threats.
- The first part of the cyber security risk management process is a ***cyber risk assessment***.
- This risk assessment will provide a snapshot of the threats that might compromise your organisation's cyber security and how severe they are.
- Based on your organisation's risk appetite, your cyber risk management programmed then determines how to priorities and respond to those risks

# What is a cyber security risk assessment?

- A cyber security risk assessment is the process of **identifying**, **analysing** and **evaluating risk**.
- It helps to ensure that the cyber security controls you choose are appropriate to the risks your organisation faces.
- A cyber security risk assessment identifies the information assets that could be affected by a cyber attack (such as hardware, systems, laptops, customer data and intellectual property). It then identifies the risks that could affect those assets.

**Aims: reduce the risk of cyber-attacks and protect against the unauthorised exploitation of systems, networks, and technologies.**

# Example of Cyber Security Risk Assessment Checklist

| Threat | Vulnerability | Asset and consequences | Risk | Solution |
|---|---|---|---|---|
| System failure — overheating in server room **High** | Air conditioning system is ten years old. **High** | Servers. All services (website, email, etc.) will be unavailable for at least 3 hours. **Critical** | **High** (potential loss of $50,000 per occurrence) | Buy a new air conditioner (cost: $3,000) |
| Malicious human (interference) — distributed denial-of-service (DDoS) attack **High** | Firewall configured properly and has good DDOS mitigation. **Low** | Website. Website will be unavailable. **Critical** | **Moderate** (potential loss of $5000 per hour of downtime) | Monitor firewall |
| Natural disaster — flooding **Moderate** | Server room is on the 3rd floor. **Very low** | Servers. All services will be unavailable. **Critical** | **Very low** | No action needed |
| Accidental human interference — accidental file deletions **High** | Permissions are configured properly; IT auditing software is in place; backups are taken regularly. **Low** | All files on a file share. Critical data could be lost, but almost certainly could be restored from backup. **Moderate** | **Low** | Continue monitoring permissions changes, privileged users, and backups |

# Risk Management Action are organization

1. security control (e.g.: physical and virtual controls)
2. processes
3. procedures
4. policies
5. risk management
6. incident management
7. framework

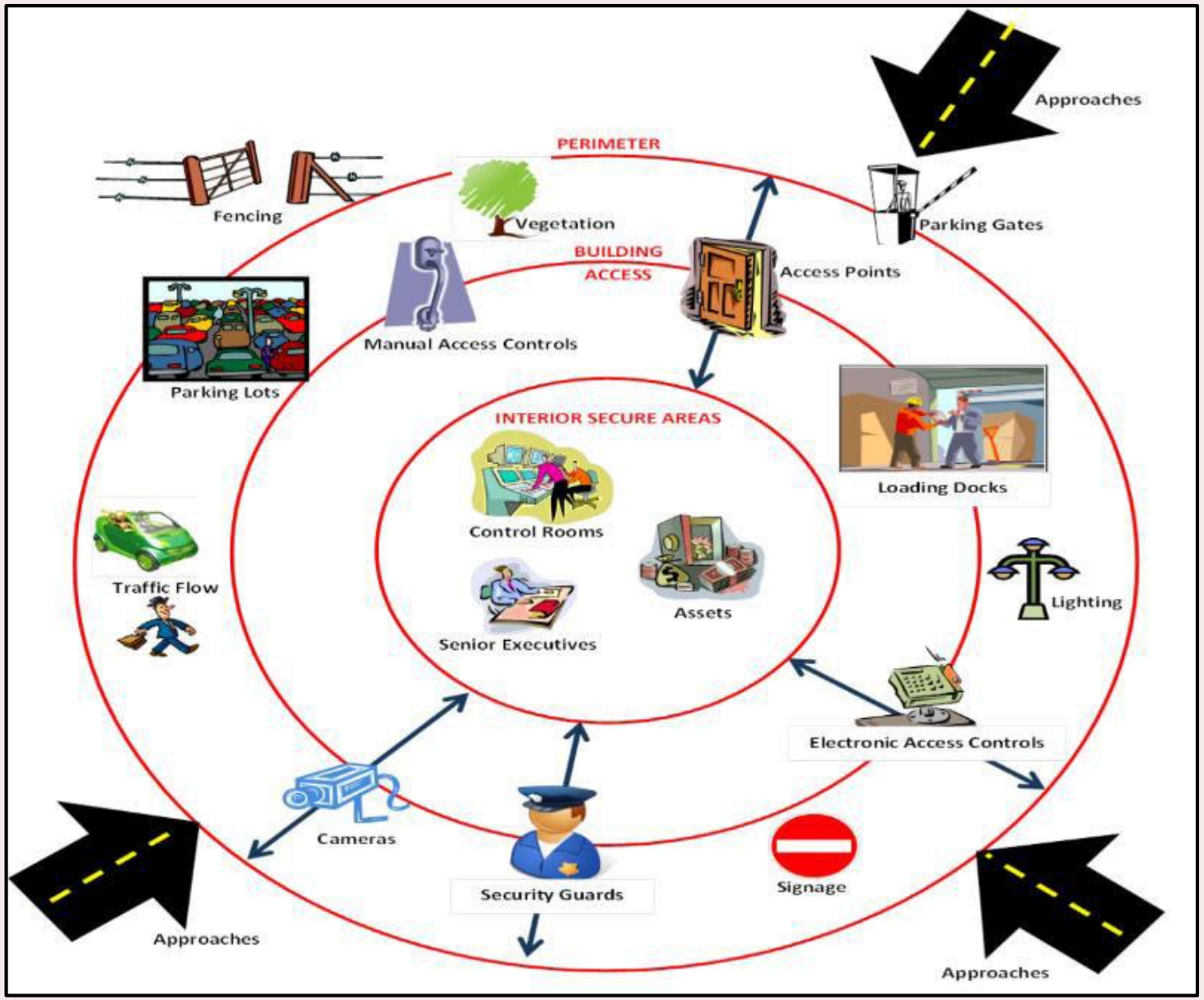
# 1. security controls

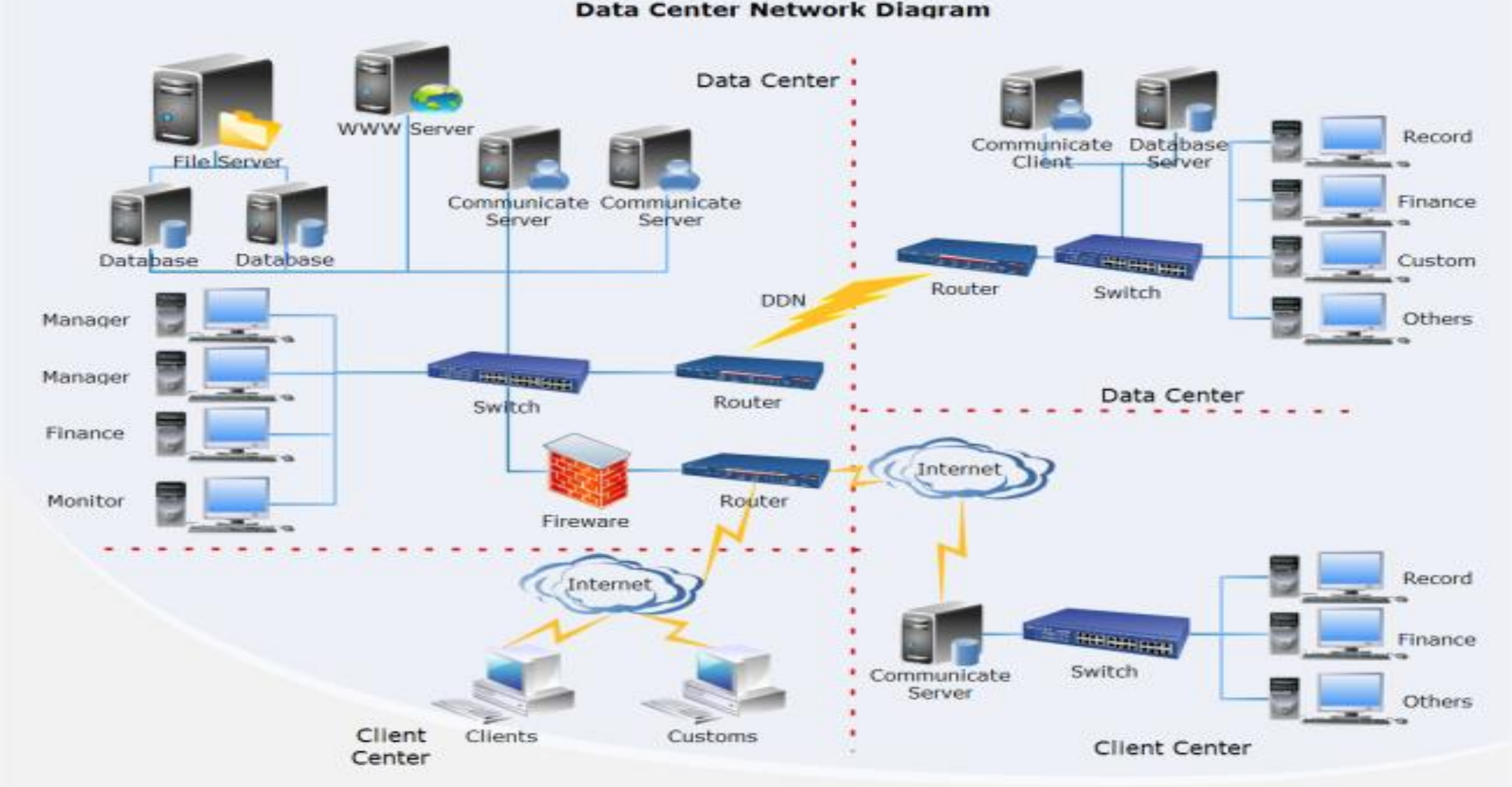
- There are three main types of IT security controls including **technical, administrative, and physical.**
- The primary goal for implementing a security control can be **preventative**, **detective**, **corrective**, **compensatory**, or act as a deterrent.
- Controls are also used to protect people as is the case with social engineering awareness training or policies.
- The lack of security controls place the confidentiality, integrity, and availability of information at risk. These risks also extend to the safety of people and assets within an organization.

**TECHNICAL CONTROLS**

**ADMINISTRATIVE CONTROLS**

**PHYSICAL CONTROLS**


Approaches
PERIMETER
Fencing
Vegetation
Parking Gates
BUILDING ACCESS
Access Points
Manual Access Controls
Parking Lots
INTERIOR SECURE AREAS
Loading Docks
Control Rooms
Traffic Flow
Assets
Lighting
Senior Executives
Electronic Access Controls
Cameras
Security Guards
Signage
Approaches
Approaches


Data Center Network Diagram
Data Center
File Server
WWW Server
Communicate Server
Communicate Server
Database
Database
Communicate Client
Database Server
Record
Finance
Custom
Others
Router
Switch
DDN
Manager
Manager
Finance
Monitor
Switch
Router
Data Center
Fireware
Router
Internet
Internet
Communicate Server
Switch
Record
Finance
Others
Client Center
Clients
Customs
Client Center

# TYPES OF SECURITY CONTROLS

## CONTROL FUNCTIONS

| | PREVENTATIVE | DETECTIVE | CORRECTIVE |
|---|---|---|---|
| PHYSICAL CONTROLS | • Fences<br>• Gates<br>• Locks | • CCTV<br>• Surveillance Cameras | • Repair physical damage<br>• Re-issue access cards |
| TECHNICAL CONTROLS | • Firewall<br>• IPS<br>• MFA<br>• Antivirus | • IDS<br>• Honeypots | • Vulnerability patching<br>• Reboot a system<br>• Quarantine a virus |
| ADMINISTRATIVE CONTROLS | • Hiring & termination policies<br>• Separation of duties<br>• Data classification | • Review access rights<br>• Audit logs and unauthorized changes | • Implement a business continuity plan<br>• Have an incident response plan |

| Technical Security Controls | Administrative Security Controls | Physical Security Controls |
|---|---|---|
| At the most basic level, technical controls, also known as logic controls, use technology to reduce vulnerabilities in hardware and software. Automated software tools are installed and configured to protect these assets. | Administrative security controls refer to policies, procedures, or guidelines that define personnel or business practices in accordance with the organization's security goals. | Physical controls are the implementation of security measures in a defined structure used to deter or prevent unauthorized access to sensitive material. |
| ❑ Encryption<br>❑ Antivirus And Anti-Malware Software<br>❑ Firewalls<br>❑ Security Information And Event Management (SIEM)<br>❑ Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) | The processes that monitor and enforce the administrative controls are:<br>❑ Management controls<br>❑ Operational controls | Examples of physical controls are:<br>❑ Closed-circuit surveillance cameras<br>❑ Motion or thermal alarm systems<br>❑ Security guards<br>❑ Picture IDs<br>❑ Locked and dead-bolted steel doors<br>❑ Biometrics (includes fingerprint, voice, face, iris, handwriting, and other automated methods used to recognize individuals) |

# 2. Risk Management Processes

**The cybersecurity risk management process involves four stages:**

- **Identifying risk** – evaluating the organization's environment to identify current or potential risks that could affect business operations
- **Assess risk** – analyzing identified risks to see how likely they are to impact the organization, and what the impact could be
- **Control risk** – define methods, procedures, technologies, or other measures that can help the organization mitigate the risks.
- **Review controls** – evaluating, on an ongoing basis, how effective controls are at mitigating risks, and adding or adjusting controls as needed.

# 3. Risk Management procedures

## An example of a Risk Management Procedure

1. Identify Cybersecurity Risks
2. Assess Cybersecurity Risks
3. Identify Possible Cybersecurity Risk Mitigation Measures
4. Collaboration and Communication Tools
5. Risk Management Frameworks
6. Analytics
7. Issues Management Tools

# An example of a Risk Management Procedure

The following, however, is an example of a risk management procedure that addresses six main areas:

1. Scope
2. Purpose
3. Reference
4. Definitions
5. Responsibilities
6. Procedure
7. Documentation

# 4. Risk Management policies

- A cybersecurity policy is a written document that contains behavioral and technical guidelines for all employees in order to ensure maximum protection from cybersecurity incidents and ransomware attacks.
- The policy contains information about a company or an organisation's security policies, procedures, technological safeguards and operational countermeasures in case of a cybersecurity incident.
- cybersecurity policy, however, can mean different things for different organisations. It can take different shapes or forms, depending on the type of organisation, nature of business, operational model, scale etc.

Here are some examples of cybersecurity policies:

1. Acceptable use policy (AUP)
2. Access control policy
3. Business continuity plan
4. Data breach response policy
5. Disaster recovery plan
6. Remote access policy

# 5. Risk Management

Today's risk landscape requires a **unified**, **coordinated**, **disciplined**, and **consistent management solution**. Below are some key risk management action components all organizations must keep in mind:

- Development of robust policies and tools to assess vendor risk
- Identification of emergent risks, such as new regulations with business impact
- Identification of internal weaknesses such as lack of two-factor authentication
- Mitigation of IT risks, possibly through training programs or new policies and internal controls
- Testing of the overall security posture
- Documentation of vendor risk management and security for regulatory examinations or to appease prospective customers

# Risk Assessment Matrix

There are many definitions of cybersecurity risk. Hence, before going further into the details of conducting a risk assessment, it is important to establish a common definition of cybersecurity risk.

For the purpose of this guidance document, risk is defined as the function of:

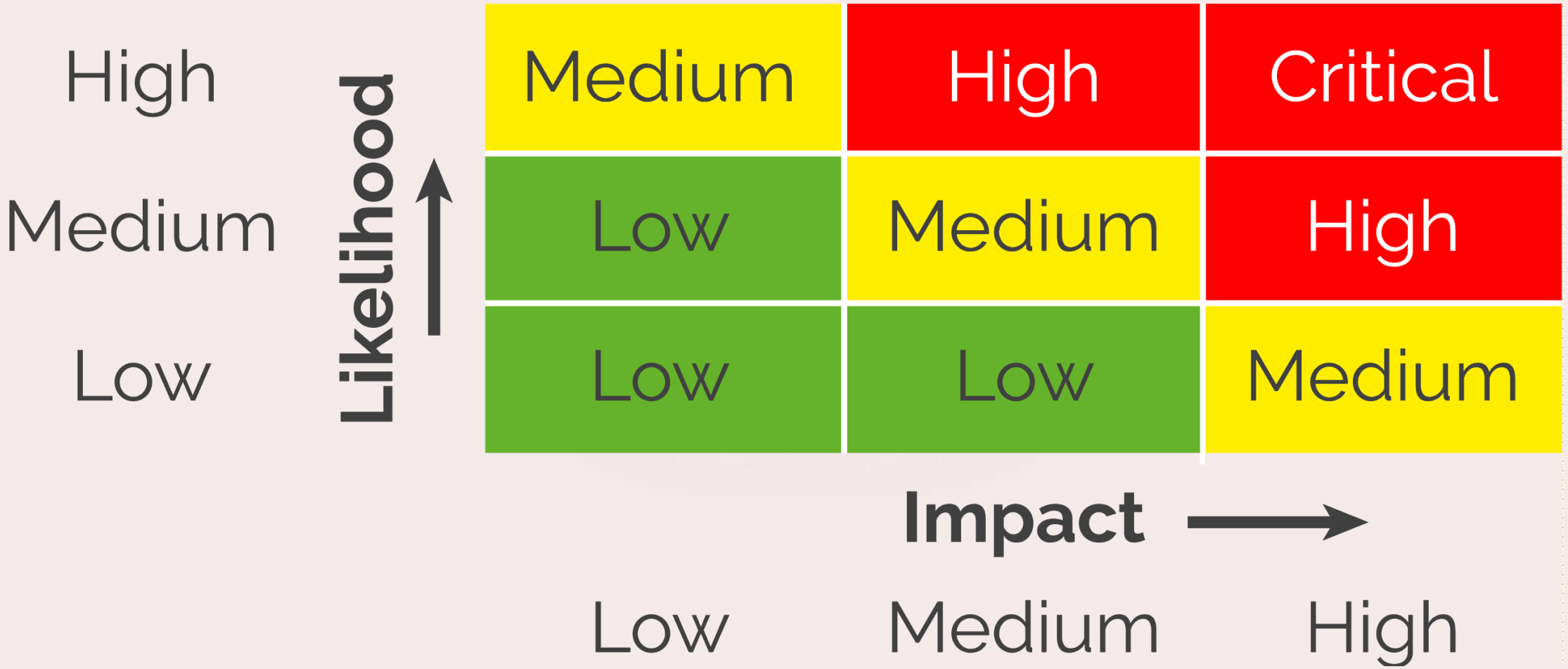
- The likelihood of a given threat event exercising on a vulnerability of an asset
- The resulting impact of the occurrence of the threat event

**Risk** = Function (**Likelihood**, **Impact**)

**Likelihood** refers to the probability that a given threat event is capable of exploiting a given vulnerability (or set of vulnerabilities). The probability can be derived based on factors namely, discoverability, exploitability and reproducibility.

**Impact** refers to the magnitude of harm resulting from a threat event exploiting a vulnerability (or set of vulnerabilities). The magnitude of harm can be estimated from the perspective of a nation, organisation, or individual.

# Risk Assessment Matrix



# Determine Risk Tolerance

| Risk Level | Risk Tolerance Description |
|---|---|
| **Very High** | This level of risk cannot be accepted and would create an impact so severe that the related activity would need to cease immediately. Alternatively, mitigation or transference strategies need to be taken immediately. |
| **High** | This level of risk cannot be accepted. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next 1 month. |
| **Medium High** | This level of risk cannot be accepted. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next 3-6 months. |
| **Medium** | This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be regularly monitored to ensure that any change in circumstance is detected and acted upon appropriately. |
| **Low** | This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be periodically monitored to ensure that any change in circumstances is detected and acted upon appropriately. |

# Risk Assessment Matrix

Impact →

Likelihood →

| | Low | Medium | High |
|---|---|---|---|
| **High** | Medium Risk (3) | High Risk (4) | Critical Risk (5) |
| **Medium** | Low Risk (2) | Medium Risk (3) | High Risk (4) |
| **Low** | Negligible Risk (1) | Low Risk (2) | Medium Risk (3) |

# 6. Incident Management

- Cybersecurity incidents can be anything from a **server outage to a data breach to something** as simple as an employee misconfiguring a firewall.
- Cybersecurity incident management aims to minimize the impact of these incidents on business operations and prevent them from happening again.
- To do this, incident managers must first identify the cause of the incident and take steps to fix it.

# What Are the Benefits of an Incident Management Plan?

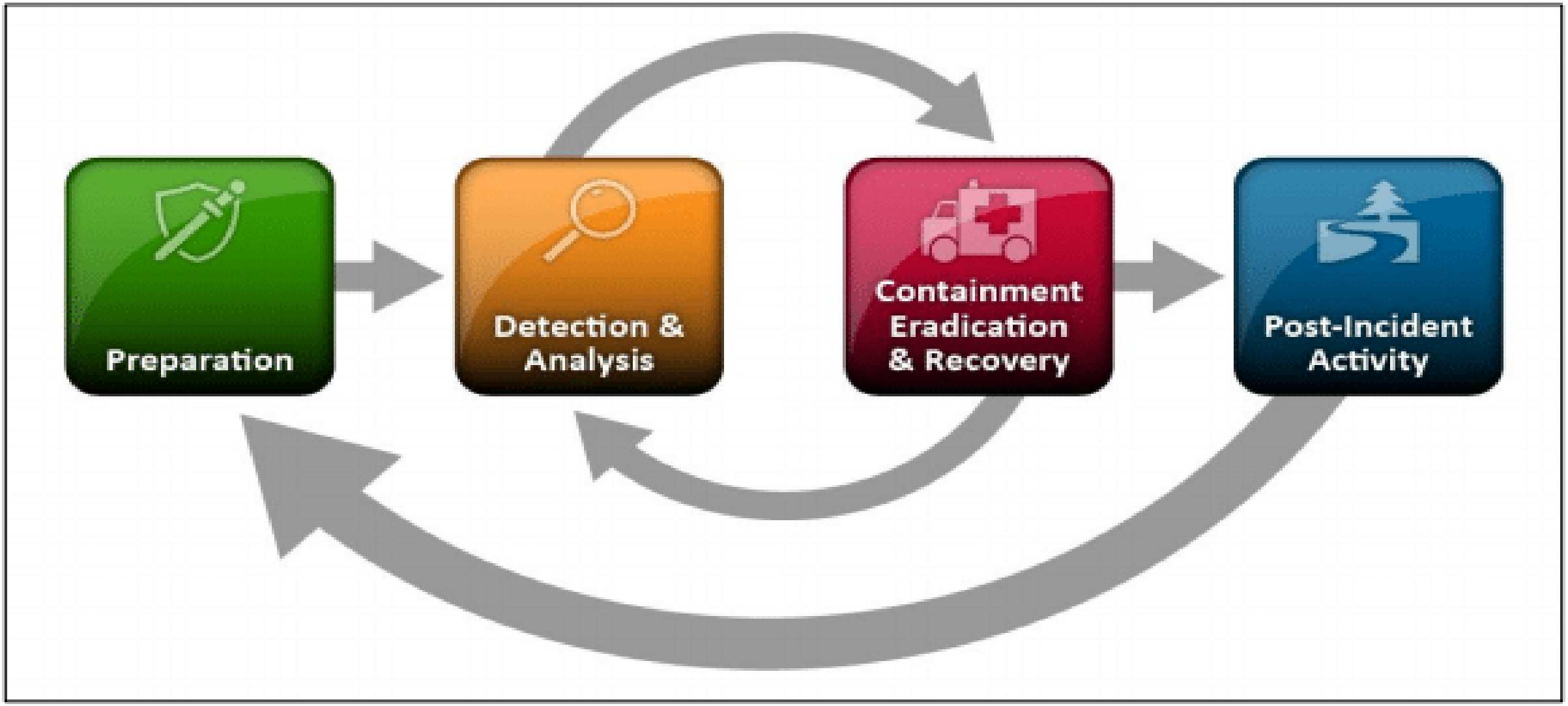
There are many benefits to implementing an effective incident management process.

- **Reduced downtime.** By quickly identifying and resolving incidents, businesses can minimize the downtime their employees experience. This is especially important for companies that rely on technology to do their work.
- **Improved customer service.** If an incident affects customers, companies must resolve the issue as soon as possible. Incident management can help businesses do this properly and efficiently.
- **Prevention of future incidents.** By identifying the root cause of incidents and fixing them, companies can prevent the same types of incidents from happening again.
- **Improved communication.** One of the critical purposes of incident management is to enhance communication between different departments and teams within an organization. Good communication prevents duplication of efforts and ensures that everyone is on the same page when responding to incidents.

# How to Create an Effective Incident Management Plan

- **Define the roles and responsibilities of the team.** Ensure everyone on the team knows their role and what they need to do to resolve an incident.
- **Establish procedures.** Make sure that you have clear procedures for responding to different types of security incidents. This will help ensure that everyone is on the same page when resolving an incident.
- **Train employees.** Train security and other staff to recognize and respond to various incidents. This will help get the business back up and running with as little downtime as possible.
- **Create a communication plan.** Make sure you have a communication plan and incident response policy in place for sharing information about incidents with employees, customers, and partners.
- **Test your plan.** Testing your plan regularly ensures that it runs smoothly, functions effectively, and is updated to account for new developments in business operations and cybersecurity.

# The NIST Incident Response Life Cycle



# 7. Risk Management framework

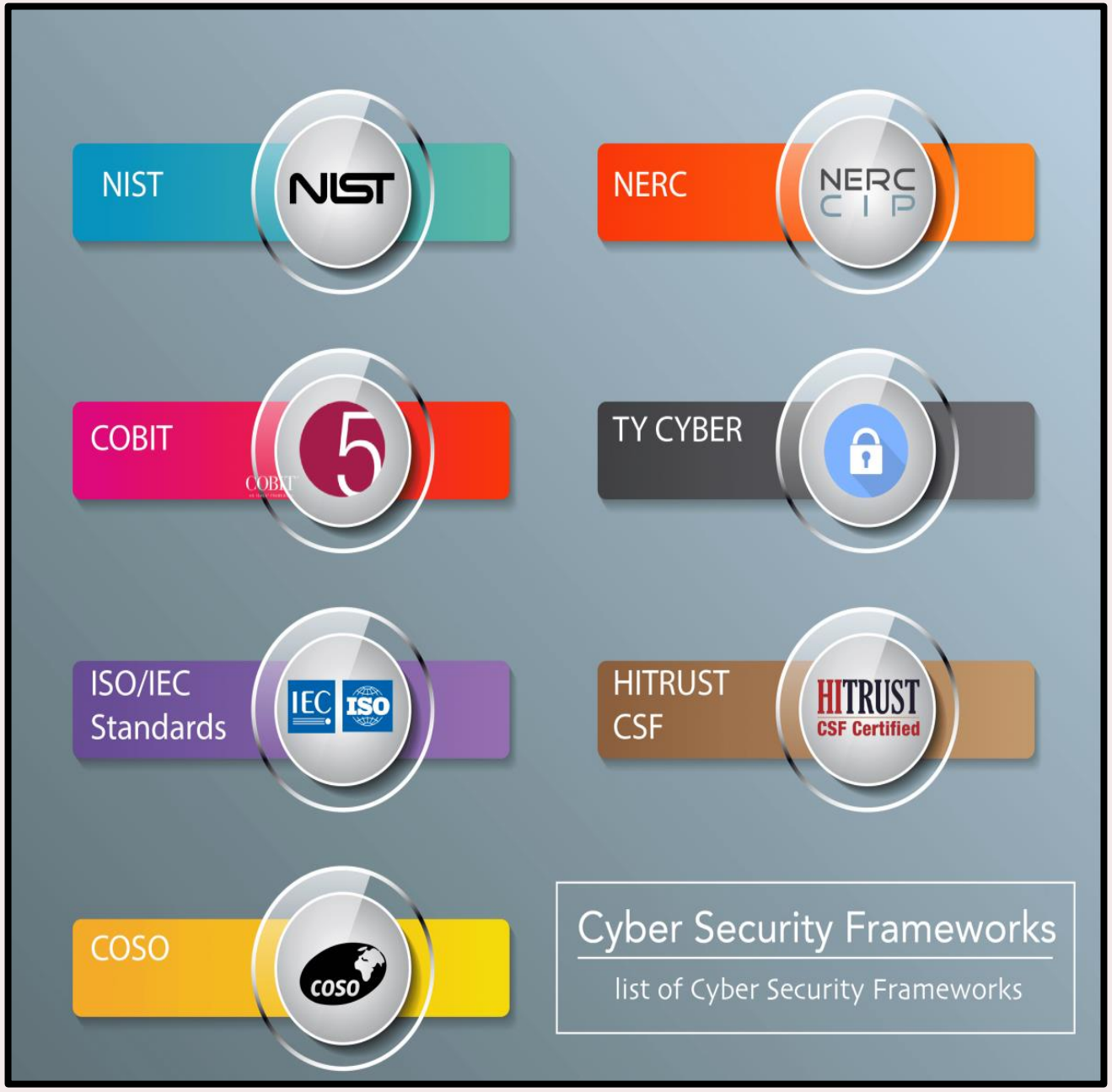
- There are several cyber risk management frameworks, each of which provides standards organizations can use to identify and mitigate risks.
- A cyber risk management framework can help organizations effectively assess, mitigate, and monitor risks; and define security processes and procedures to address them.

**Examples of some cyber security management framework standards bodies are** :

1. The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) is a popular framework.
2. The International Organization for Standardization (ISO) has created the ISO/IEC 270001 in partnership with the International Electro technical Commission (IEC).

# NIST Risk Management Framework


- The Risk Management Framework provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle.
- The risk-based approach to control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations.


NIST
NERC
COBIT
TY CYBER
ISO/IEC
Standards
HITRUST
CSF
COSO
Cyber Security Frameworks
list of Cyber Security Frameworks

# NIST Cybersecurity Framework

| IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER |
|---|---|---|---|---|
| • Asset Management<br>• Business Environment<br>• Governance<br>• Risk Assessment<br>• Risk Management Strategy | • Awareness Control<br>• Awareness and Training<br>• Data Security<br>• Info Protection and Procedures<br>• Maintenance<br>• Protective Technology | • Anomalies and Events<br>• Continuous Security Monitoring<br>• Detection Process | • Response Planning<br>• Communications<br>• Analysis<br>• Mitigation<br>• Improvements | • Recovery Planning<br>• Improvements<br>• Communications |

| Capability | Description |
| --- | --- |
| Identify | What processes and assets need protection? |
| Protect | Implement appropriate safeguards to ensure protection of the enterprise's assets |
| Detect | Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents |
| Respond | Develop techniques to contain the impacts of cybersecurity events |
| Recover | Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events |

# Thank You!

## Lesson Two Completed!

U Tin Naing Htwe
Senior Lecturer(ICT)
Optimum Institute