

INTRODUCTION TO CYBER SECURITY FRAMEWORKS & STANDARDS

Presented By:
Prashant Saxena
IT Engineer

Rajasthan Rajya Vidyut Prasaran Nigam Limited
(RAJASTHAN TRANSCO)

Certified ISO 27001:2013 Lead Auditor
Author of “ Cyber Security – The Fourth
Dimension in Post covid World”



TODAYS ROADMAP TO CYBER SECURITY FRAMEWORKS

NIST(National Institute of Standards and Technology) Cyber Security Framework

Introduction to ISO 2700:2013

Risk Assessment in ISMS

Vulnerability Assessment

WHAT IS INFORMATION?

Information is a basic building block of any organization.

Information is more than electronically stored or processed data. Information can be :

- ❖ Created
- ❖ Stored
- ❖ Destroyed
- ❖ Processed
- ❖ Transmitted
- ❖ Used
- ❖ Lost
- ❖ Corrupted

BENEFITS OF AN INFORMATION SECURITY TO THE ORGANIZATION

After implementing an ISMS, the organization may realize the benefits of:

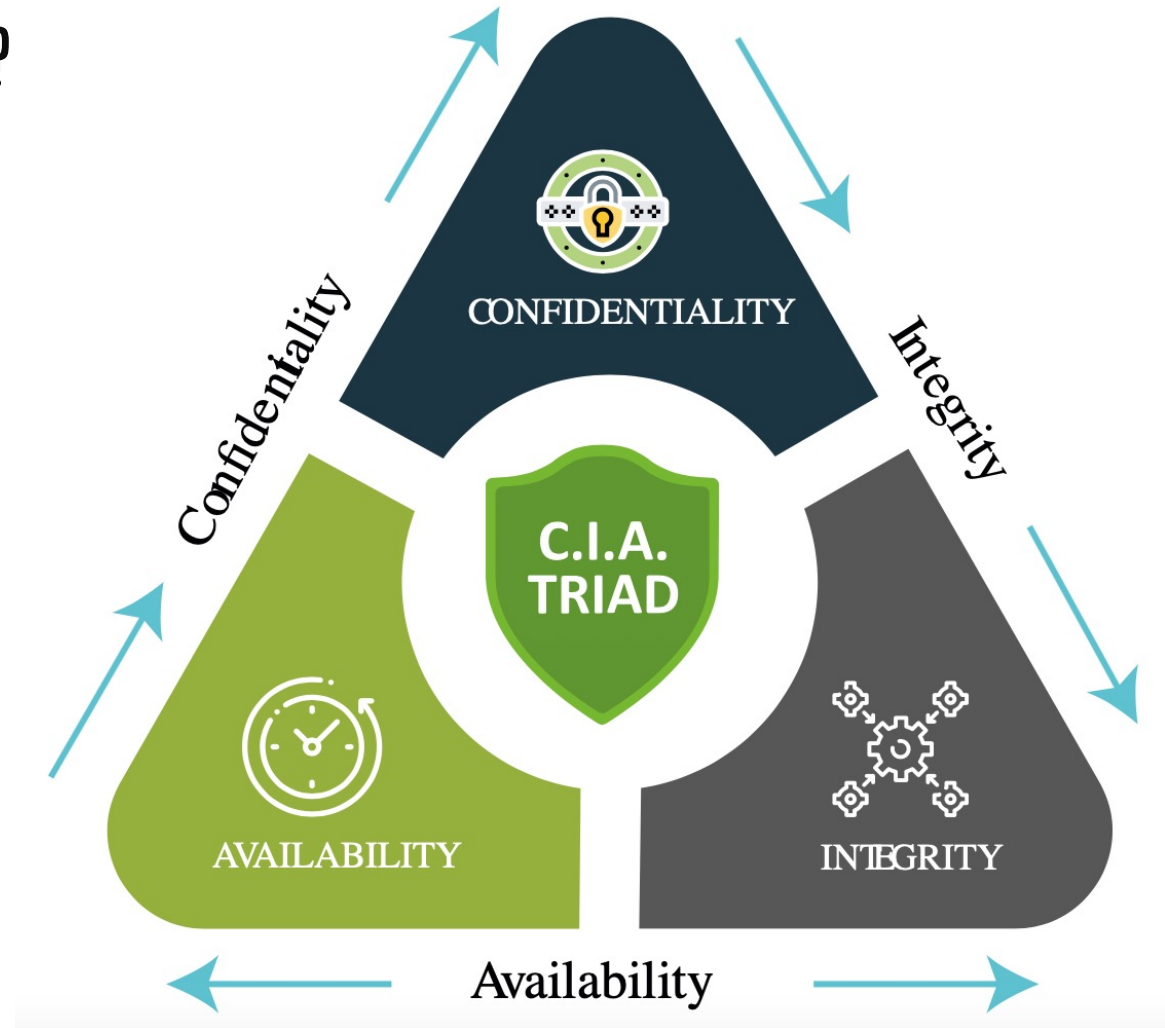
- preventing an information security incident from occurring
- reducing the likelihood of a security incident occurring;
- detecting an incident occurring, or its effects;
- protecting the information from the effects of an incident;
- responding to an incident to minimize business damage
- recovering quickly should an incident occur.
- reducing the consequences or impact of a security incident

WHAT IS INFORMATION SECURITY?

In business, having the correct information to the authorized person at the right time can make the difference between profit and loss, success and failure.

There are three main aspects of information security:

1. Confidentiality: Protecting information from unauthorized disclosure, perhaps to a competitor or to press
2. Integrity: Protecting information from unauthorized modification, and ensuring that information, such as price list, is accurate and complete
3. Availability: Ensuring information is available when you need it, such as to get access to data after disaster.



WHAT IS A FRAMEWORK?

Cyber security frameworks are sets of documents describing guidelines, standards, and best practices designed for cyber security risk management.

The frameworks exist to reduce an organization's exposure to weaknesses and vulnerabilities that hackers and other cyber criminals may exploit.



NIST CYBER SECURITY FRAMEWORK

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes.

The Framework consists of three parts:

1. The Framework Core
2. the Implementation Tiers
3. the Framework Profiles.

SALIENT FEATURES OF FRAMEWORK

This framework was developed to improve cybersecurity risk management in critical infrastructure, the Framework can be used by organizations in any sector or community.

The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience.

The Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today.

The Framework remains effective and supports technical innovation because it is technology neutral, while also referencing a variety of existing standards, guidelines, and practices that evolve with technology

SALIENT FEATURES OF FRAMEWORK

The Framework offers a flexible way to address cybersecurity, including cybersecurity's effect on physical, cyber, and people dimensions. It is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT).

The Framework can assist organizations in addressing cybersecurity as it affects the privacy of customers, employees, and other parties. Additionally, the Framework's outcomes serve as targets for workforce development and evolution activities.

The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation.

HISTORY OF NIST FRAMEWORK ON CYBER SECURITY

To strengthen the resilience of this infrastructure, the Cybersecurity Enhancement Act of 2014² (CEA) updated the role of the National Institute of Standards and Technology (NIST) to “facilitate and support the development of” cybersecurity risk frameworks. Through CEA, NIST must identify “a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks.”

This formalized NIST’s previous work developing Framework Version 1.0 under Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” issued in February 2013³, and provided guidance for future Framework evolution.

WHY ANY ORGANIZATION ADOPT THIS FRAMEWORK?

Describe their current cybersecurity posture

Describe their target state for cybersecurity

Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process

Assess progress toward the target state

Communicate among internal and external stakeholders about cybersecurity risk

OVERVIEW OF THE FRAMEWORK

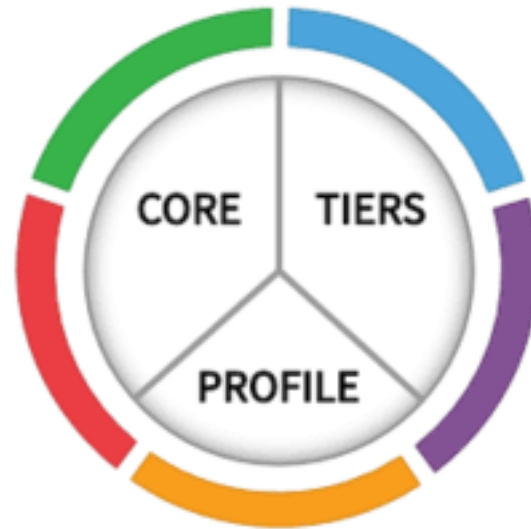
The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles.

Each Framework component reinforces the connection between business/mission drivers and cybersecurity activities.

The Framework provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders.

It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk

THREE BASIC COMPONENTS OF FRAMEWORK



A. FRAMEWORK CORE

The *Framework Core* provides a set of activities to achieve specific cybersecurity *outcomes*, and references examples of guidance to achieve those outcomes.

The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by stakeholders as helpful in managing cybersecurity risk.

The Core comprises four elements: Functions, Categories, Subcategories, and Informative References.

FRAMEWORK CORE STRUCTURE

FRAMEWORK FUNCTIONS	IDENTIFY ID	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
	PROTECT PR	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
	DETECT DE	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
	RESPOND RS	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
	RECOVER RC	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES

FRAMEWORK CORE ELEMENT- FUNCTION

Functions organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover.

They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.

The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services.

FRAMEWORK CORE ELEMENT- CATEGORIES

Categories are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Identity Management and Access Control,” and “Detection Processes.”

FRAMEWORK CORE ELEMENT- SUBCATEGORIES

Subcategories further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”

FRAMEWORK CORE ELEMENT- INFORMATIVE REFERENCES

Informative References are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process.

FRAMEWORK CORE FUNCTIONS

These Functions are not intended to form a serial path or lead to a static desired end state.

The Functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk



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

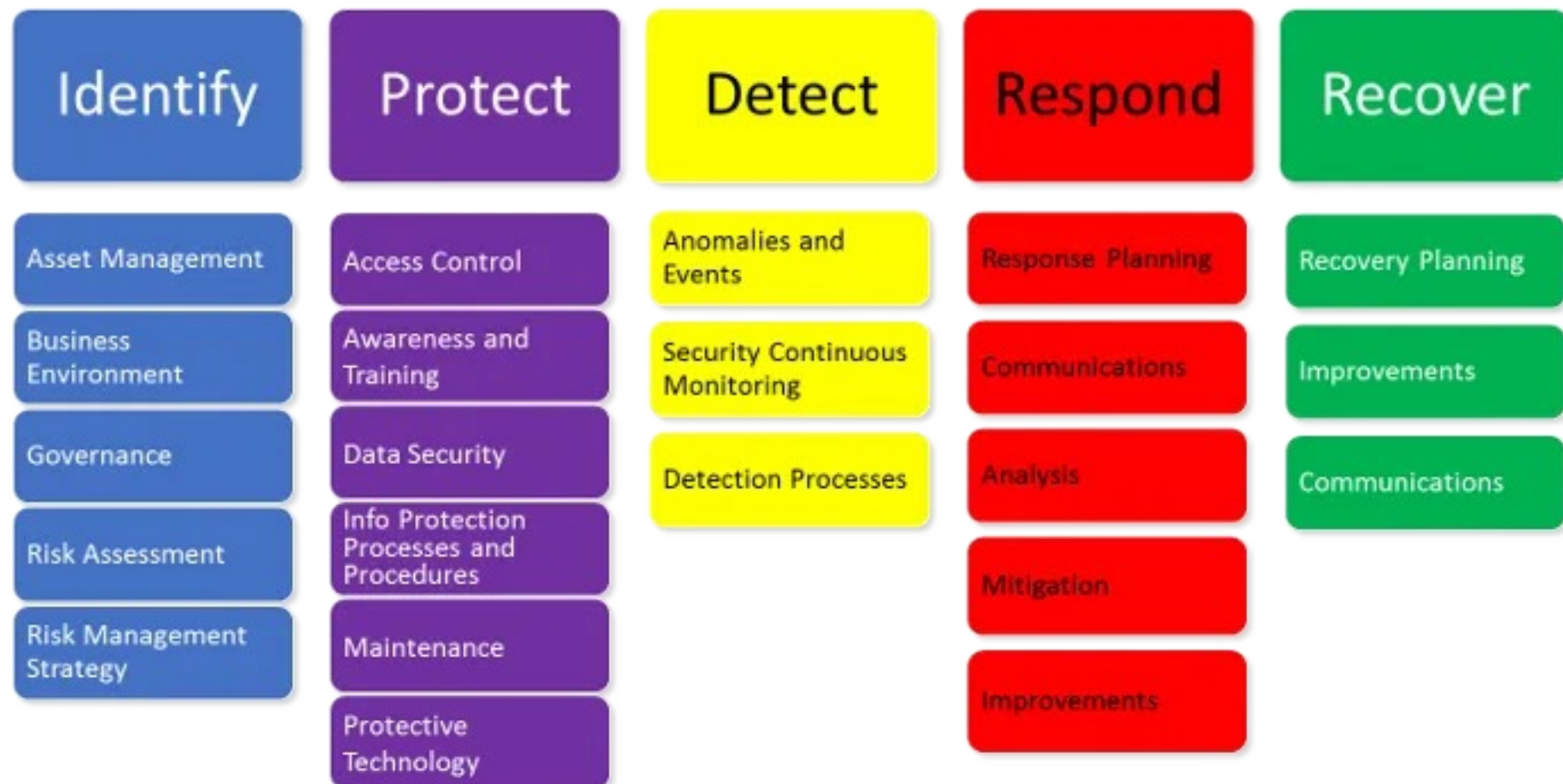
Respond

Develop techniques to contain the impacts of cybersecurity events

Recover

Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events

NIST Cyber Security Framework



1. IDENTIFY

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	CIS CSC 17, 19 COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03

2. PROTECT

Develop and implement appropriate safeguards to ensure delivery of critical services.

The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

PROTECT (PR)

Identity Management, Authentication and Access Control (PR.AC): Access to 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.

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

CIS CSC 1, 5, 15, 16
COBIT 5 DSS05.04, DSS06.03
ISA 62443-2-1:2009 4.3.3.5.1
ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3
NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11

PR.AC-2: Physical access to assets is managed and protected

COBIT 5 DSS01.04, DSS05.05
ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8
ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8
NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8

PR.AC-3: Remote access is managed

CIS CSC 12
COBIT 5 APO13.01, DSS01.04, DSS05.03
ISA 62443-2-1:2009 4.3.3.6.6
ISA 62443-3-3:2013 SR 1.13, SR 2.6
ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1

3. DETECT

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

The Detect Function enables timely discovery of cybersecurity events.

Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected	DE.AE-1: A baseline of network operations and expected data flows for	CIS CSC 1, 4, 6, 12, 13, 15, 16 COBIT 5 DSS03.01 ISA 62443-2-1:2009 4.4.3.3
	and the potential impact of events is understood.	users and systems is established and managed	ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	CIS CSC 3, 6, 13, 15 COBIT 5 DSS05.07 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 COBIT 5 BAI08.02 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1, A.16.1.7 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	CIS CSC 4, 6 COBIT 5 APO12.06, DSS03.01 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Incident alert thresholds are established	CIS CSC 6, 19 COBIT 5 APO12.06, DSS03.01 ISA 62443-2-1:2009 4.2.3.10 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify	DE.CM-1: The network is monitored to detect potential cybersecurity events	CIS CSC 1, 7, 8, 12, 13, 15, 16 COBIT 5 DSS01.03, DSS03.05, DSS05.07 ISA 62443-3-3:2013 SR 6.2 NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4

4. RESPOND

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.

Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

Function	Category	Subcategory	Informative References
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	RS.RP-1: Response plan is executed during or after an incident	CIS CSC 19 COBIT 5 APO12.06, BAI01.10 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-1: Personnel know their roles and order of operations when a response is needed	CIS CSC 19 COBIT 5 EDM03.02, APO01.02, APO12.03 ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1 NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Incidents are reported consistent with established criteria	CIS CSC 19 COBIT 5 DSS01.03 ISA 62443-2-1:2009 4.3.4.5.5 ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	CIS CSC 19 COBIT 5 DSS03.04 ISA 62443-2-1:2009 4.3.4.5.2 ISO/IEC 27001:2013 A.16.1.2, Clause 7.4, Clause 16.1.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	CIS CSC 19 COBIT 5 DSS03.04 ISA 62443-2-1:2009 4.3.4.5.5 ISO/IEC 27001:2013 Clause 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	CIS CSC 19 COBIT 5 BAI08.04 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15

5. RECOVER

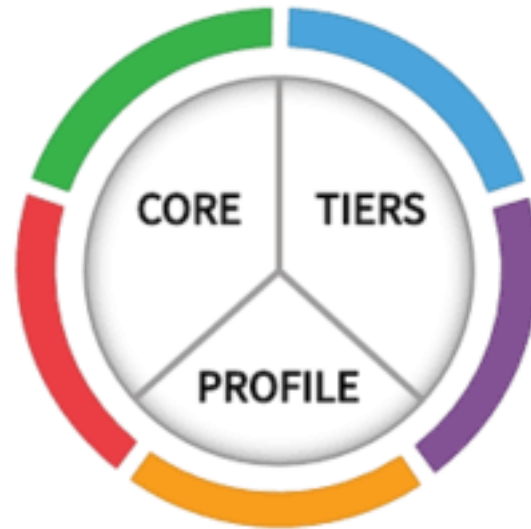
Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	CIS CSC 10 COBIT 5 APO12.06, DSS02.05, DSS03.04 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	COBIT 5 APO12.06, BAI05.07, DSS04.08 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	COBIT 5 APO12.06, BAI07.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

THREE BASIC COMPONENTS OF FRAMEWORK



B. FRAMEWORK IMPLEMENTATION TIERS

The Framework Implementation Tiers (“Tiers”) provide context on how an organization views cybersecurity risk and the processes in place to manage that risk.

Ranging from Partial (Tier 1) to Adaptive (Tier 4), Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices.

They help determine the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization’s overall risk management practices.

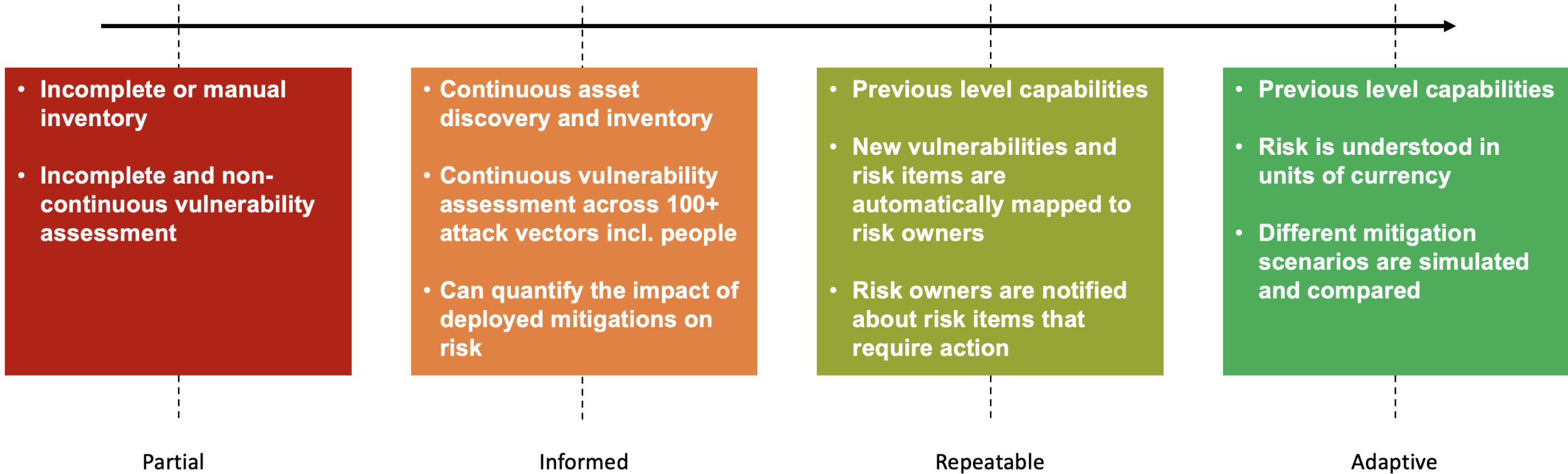
Risk management considerations include many aspects of cybersecurity, including the degree to which privacy and civil liberties considerations are integrated into an organization’s management of cybersecurity risk and potential risk responses.

TIER SELECTION

The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, information sharing practices, business/mission objectives, supply chain cybersecurity requirements, and organizational constraints.

Organizations should determine the desired Tier, ensuring that the selected level meets the organizational goals, is feasible to implement, and reduces cybersecurity risk to critical assets and resources to levels acceptable to the organization.

While organizations identified as Tier 1 (Partial) are encouraged to consider moving toward Tier 2 or greater, Tiers do not represent maturity levels. Tiers are meant to support organizational decision making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and could receive additional resources



TIER 1: PARTIAL

Risk Management Process – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner.

Integrated Risk Management Program – There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources.

External Participation – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information.

TIER 2: RISK INFORMED

Risk Management Process – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.

Integrated Risk Management Program – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis..

External Participation – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others

TIER 3: REPEATABLE

Risk Management Process – The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.

Integrated Risk Management Program – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed.

External Participation - It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities.

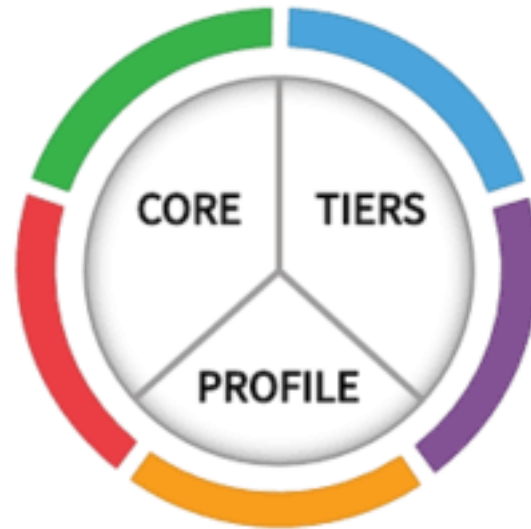
TIER 4: ADAPTIVE

Risk Management Process – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. The organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving, sophisticated threats.

Integrated Risk Management Program – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.

External Participation - It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators.

THREE BASIC COMPONENTS OF FRAMEWORK



C. FRAMEWORK PROFILE

The Framework Profile (“Profile”) is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization.

A Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities.

Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs.

FRAMEWORK PROFILE

Framework Profiles can be used to describe the current state or the desired target state of specific cybersecurity activities.

The Current Profile indicates the cybersecurity outcomes that are currently being achieved.

The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. Profiles support business/mission requirements and aid in communicating risk within and between organizations.

The Framework does not prescribe Profile templates, allowing for flexibility in implementation.



ESTABLISHING OR IMPROVING A CYBERSECURITY PROGRAM

Steps illustrate how an organization could use the Framework to create a new cybersecurity program or improve an existing program. These steps should be repeated as necessary to continuously improve cybersecurity.

- 1. Prioritize and Scope.**
- 2. Orient**
- 3. Create a Current Profile**
- 4. Conduct a Risk Assessment**
- 5. Create a Target Profile**
- 6. Determine, Analyse, and Prioritize Gaps**
- 7. Implement Action Plan**

STEP 1: PRIORITIZE AND SCOPE

The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.

STEP 2: ORIENT

Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.

STEP 3: CREATE A CURRENT PROFILE

The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

STEP 4: CONDUCT A RISK ASSESSMENT

This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization.

It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

STEP 5: CREATE A TARGET PROFILE

The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

STEP 6: DETERMINE, ANALYZE, AND PRIORITIZE GAPS

The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile.

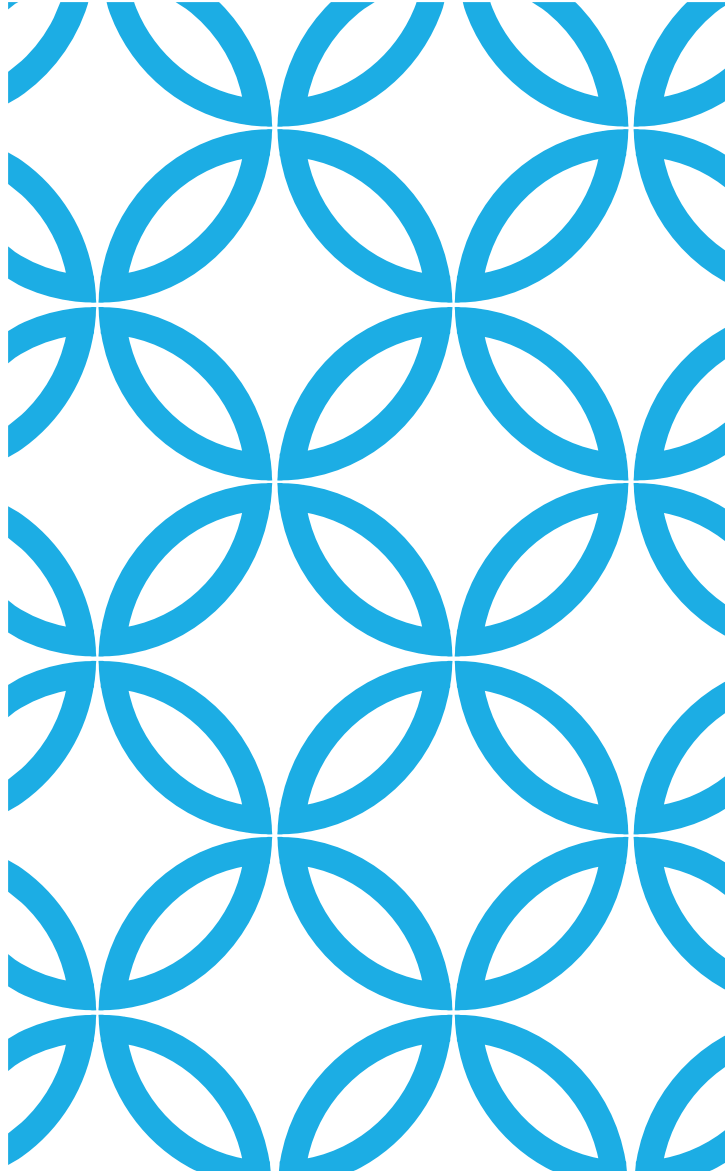
The organization then determines resources, including funding and workforce, necessary to address the gaps.

Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

STEP 7: IMPLEMENT ACTION PLAN

The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile.

The Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.



ISO 27001:2013- ISMS

CURRENT SCENARIO

Present day organizations are highly dependent on information systems to manage business and deliver products/services.

Dependence on IT for development, production and delivery in various internal applications like

- Financial databases.
- Employee time booking.
- Providing helpdesk and other services.
- Providing remote access to customers/employees.
- Remote access of client systems.
- Interactions with the outside world through e-mail, internet.

THREATS

If Information Security is not addressed, then there are chances of various threats occurring like:

Fraud

Surveillance

Sabotage- Disrupt Services

Destruction

Fire

Flood



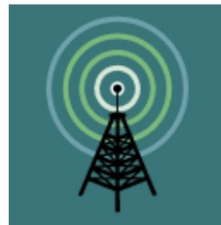
High User Knowledge
of IT Systems



Theft, Sabotage,
Misuse



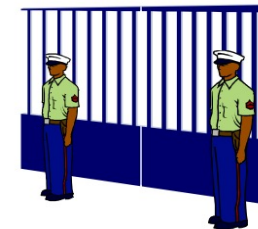
Virus Attacks



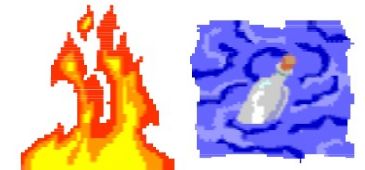
Systems and
Network Failure



Lack Of
Documentation



Lapse in Physical
Security



Natural
Calamities and
Fire

EXPLOITATION OF THREATS CAN RESULT IN FOLLOWING LOSSES

Financial loss.

Loss of sales / market share.

Service unavailability and disruption to operations.

Loss of processing capability and productivity.

Damage to image and reputation.

INFORMATION - DEFINITION

As per ISO/IEC 27000, “Information (knowledge or data) is an asset which, like other important business assets, is of value to an organization and consequently needs to be suitably protected....”

“... Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.”

WHAT IS ISMS?

ISMS is an abbreviation for Information Security Management System Definition:

Part of the overall Management System, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

Note:

The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

REQUIREMENTS AND GUIDELINES

Requirement Standard



Requirements

Auditable

Used as a basis for
certification

Guideline Standard

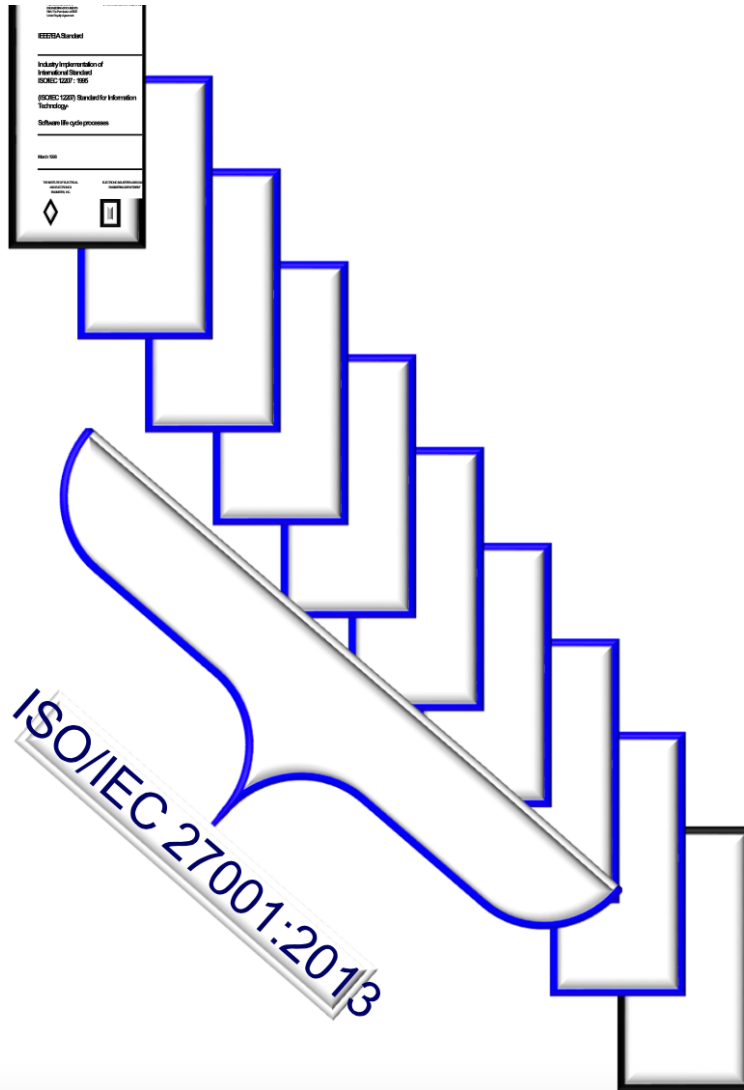


Elaborate explanation of
the requirement to aid in
understanding the
requirement.

Advisory, Best practice
guidance

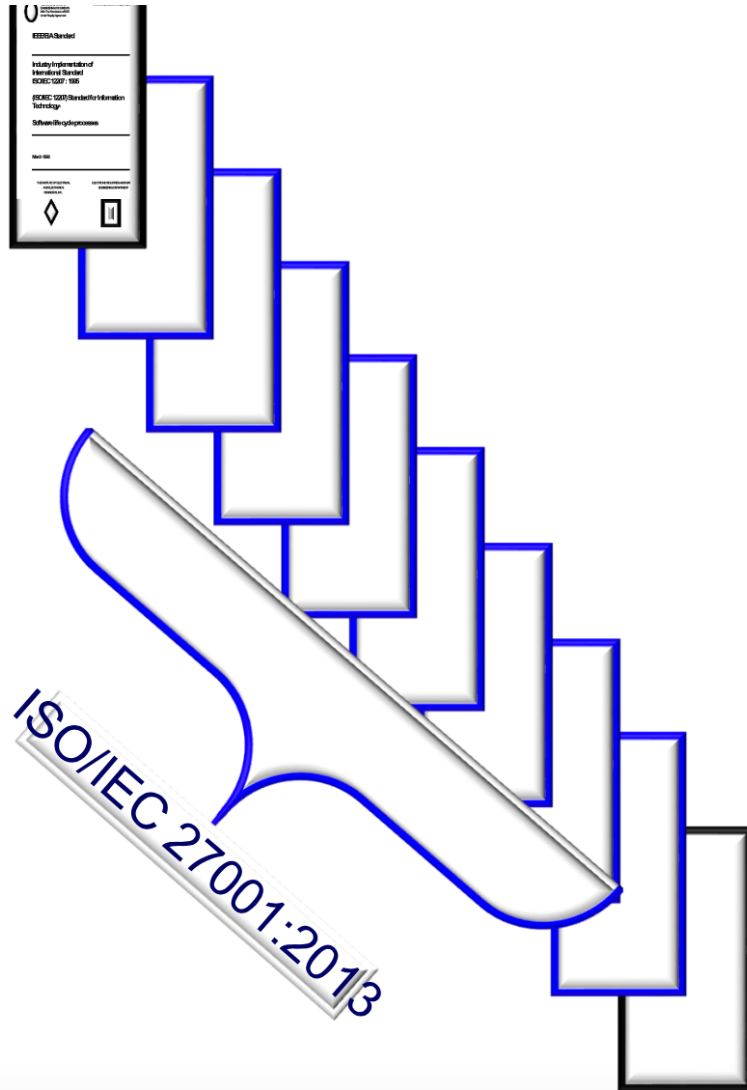
Code of Practice

ISO/IEC 27001:2013 STRUCTURE



1. **Scope**
2. **Normative References**
3. **Terms and Definitions**
4. **Context of the organization**
 - 4.1 ***Understanding the organization and its context***
 - 4.2 ***Understanding the needs and expectations of interested parties***
 - 4.3 ***Determining the scope of the information security management system***
 - 4.4 ***Information security management system***

ISO/IEC 27001:2013 STRUCTURE



5. Leadership

5.1 Leadership and commitment

5.2 Policy

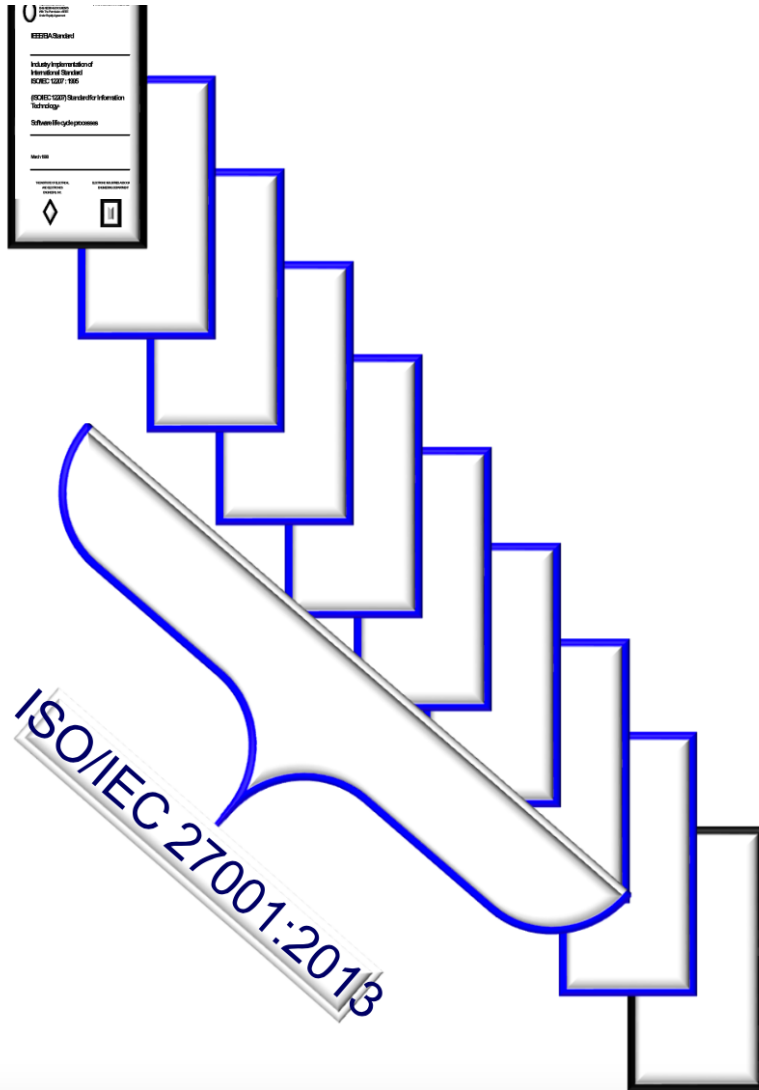
5.3 Organizational roles, responsibilities and authorities

6. Planning

6.1 Actions to address risks and opportunities

6.2 Information security objectives and planning to achieve them

ISO/IEC 27001:2013 STRUCTURE



7. Support

7.1 Resource

7.2 Competence

7.3 Awareness

7.4 Communication

7.5 Documented information

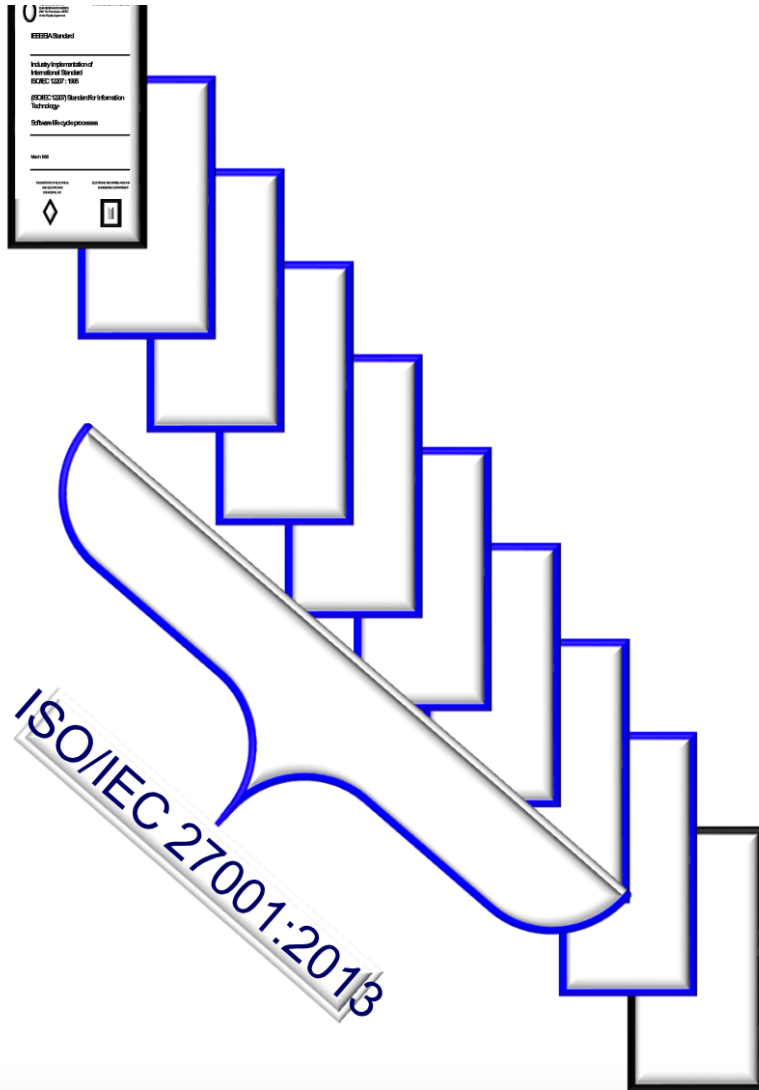
8. Operation

8.1 Operational planning and control

8.2 Information security risk assessment

8.3 Information security risk treatment

ISO/IEC 27001:2013 STRUCTURE



9. Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.2 Internal audit

9.3 Management review

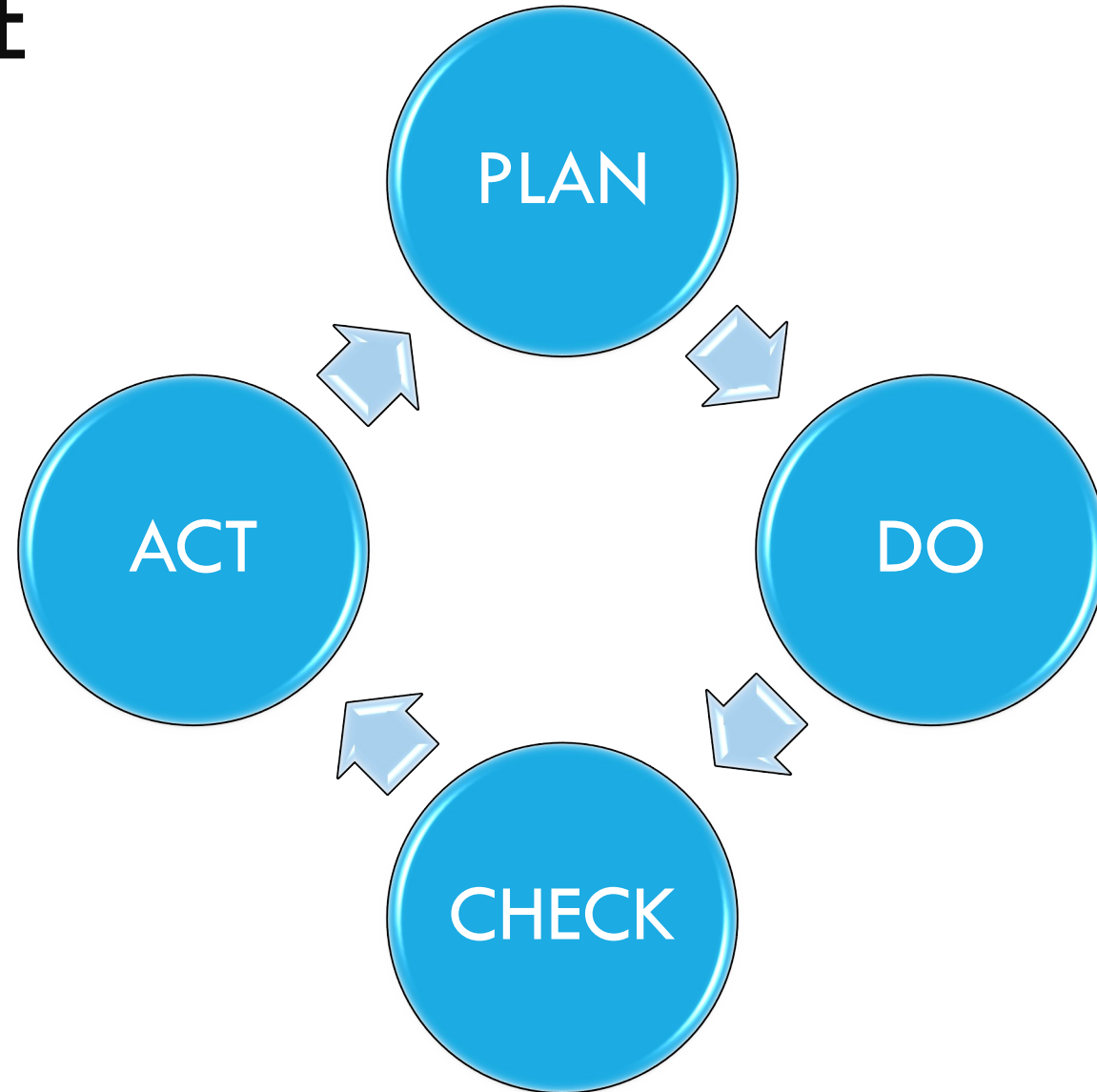
10. Improvement

10.1 Non conformity and corrective action

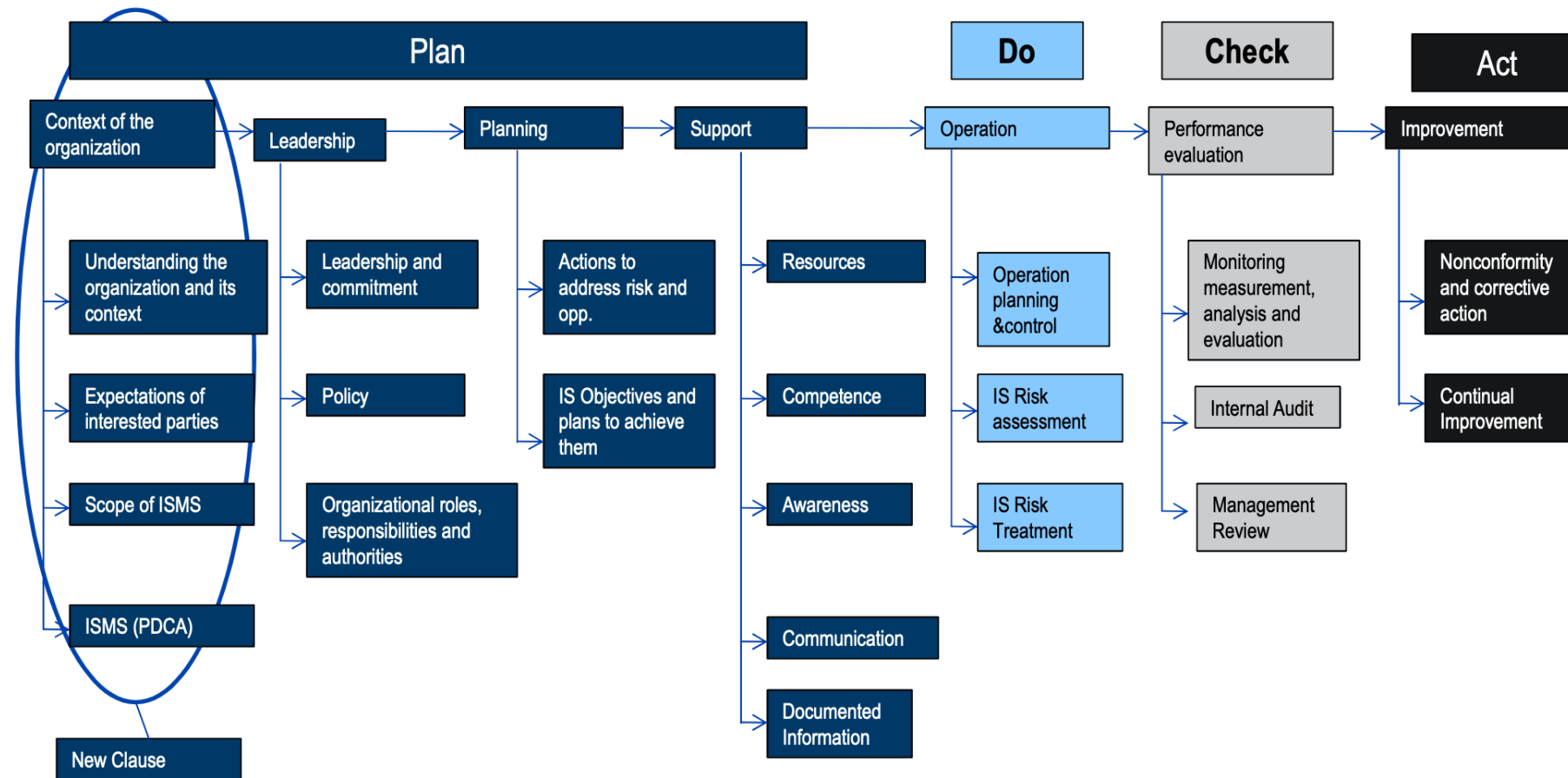
10.2 Continual improvement

Annex A (normative) Reference control objectives and controls

PDCA CYCLE



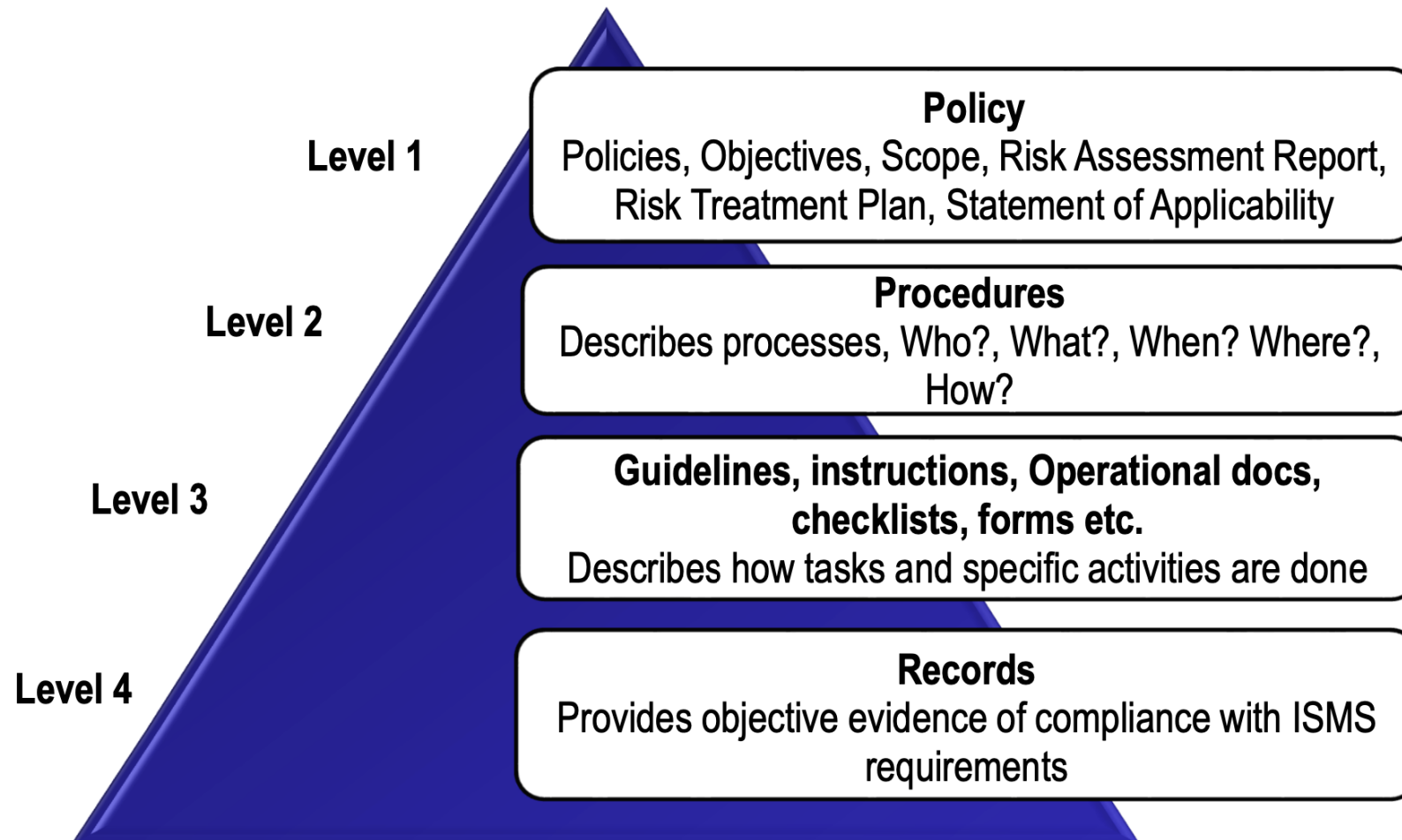
PDCA CYCLE



ISO/IEC 27001 REQUIREMENTS

Requirements contained in the ISMS Framework (Sections 4-10) -	Excluding any of the requirements specified in these clauses (4 to 10) is not acceptable when an organization claims conformity to this standard
ISMS control requirements [Annex A]-	Justify exclusions

HIERARCHICAL STRUCTURE



ISMS DOCUMENTATION



Security Policy & SoA(Statement of Applicability)- Summary of management framework including the information security policy and the control objectives and implemented controls given in the statement of applicability.



Procedures & Policy- Policy / Procedures adopted to implement the controls required.

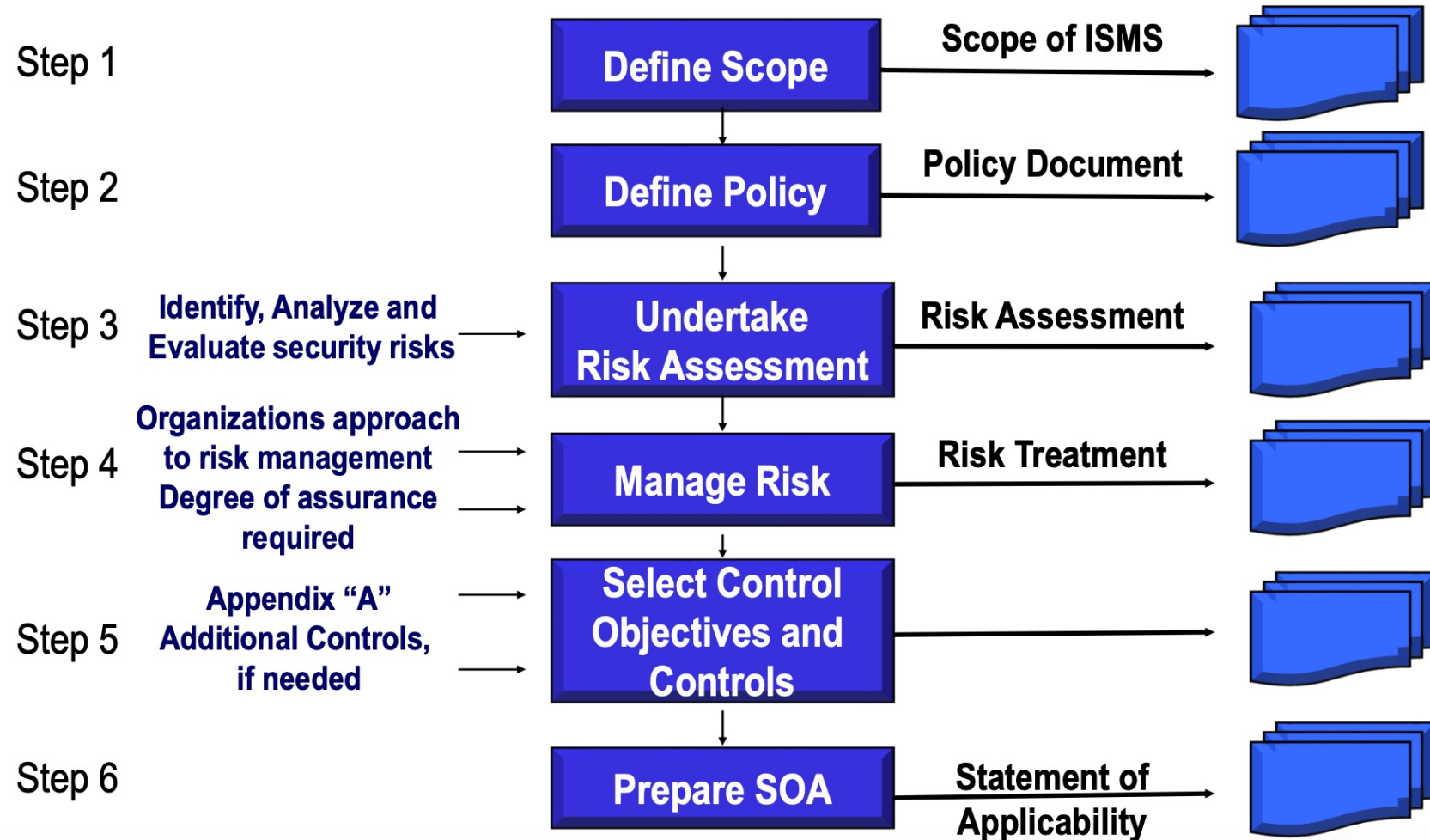


Operational Documents- Explains details of specific tasks or activities.



Records- Evidence of activities carried out.

RISK BASED APPROACH



THE PURPOSE OF RISK ASSESSMENT

To identify the security requirements for the organization's information assets.

To review the consequences of the risks i.e. impact to the business.

To make decisions on how to manage the risks

COMPONENTS OF RISK ASSESSMENT

Assets (Physical,
People, Paper,
Information, Software,
Services), Asset Name

Risk owners , Asset
owner

Asset Evaluation -
Confidentiality,
Integrity, Availability

Threats

Vulnerabilities

Probability Value
(Likelihood of
Occurrence)

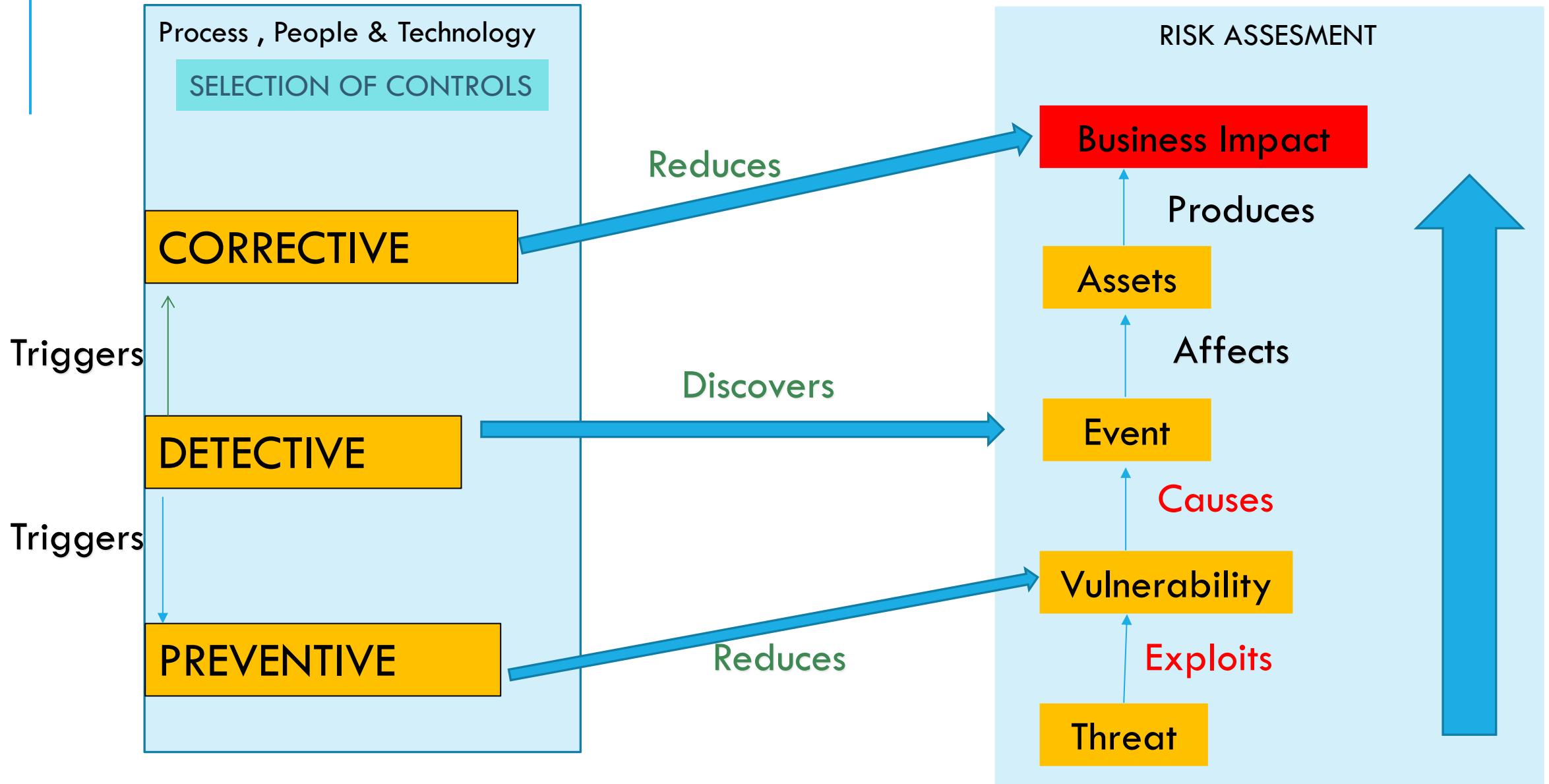
Security Controls

ASSET BASED RISK ASSESSMENT

- ❖ An **Asset** is which we are trying to protect.
- ❖ A **threat** is whome we are trying to protect against.
- ❖ A **vulnerability** is a weakness or gap in our protection efforts.
- ❖ **Risk** is the intersection of assets, threats and vulnerabilities.

ASSET X THREAT X VULNERABILITY = RISK SCORE

CONTROL RELATION WITH RISK ASSESSMENT



ASSET VALUATION

To determine the value of an asset, follow these steps

1. Identify all the information assets and determine their owner.
2. Identify the value of each of these information assets in terms of confidentiality, integrity and availability i.e. impact on the organization, partners, customers and other interested parties in the event of a breach of the confidentiality, integrity or availability of the asset
3. Ensure that the value is identified in the context in which they are used.

EXAMPLE: ASSET VALUATION

Critical	4
High	3
Medium	2
Low	1

Asset Group	Asset name	C	I	A	Max	Category
Information Assets	Backup Media	1	2	3	3	High
People Assets	HR Group	2	3	3	3	High
Physical Assets	Servers	1	2	2	2	Medium
Service Assets	Transport	1	1	1	1	Low
Software assets	MS SQL	1	1	4	4	Critical

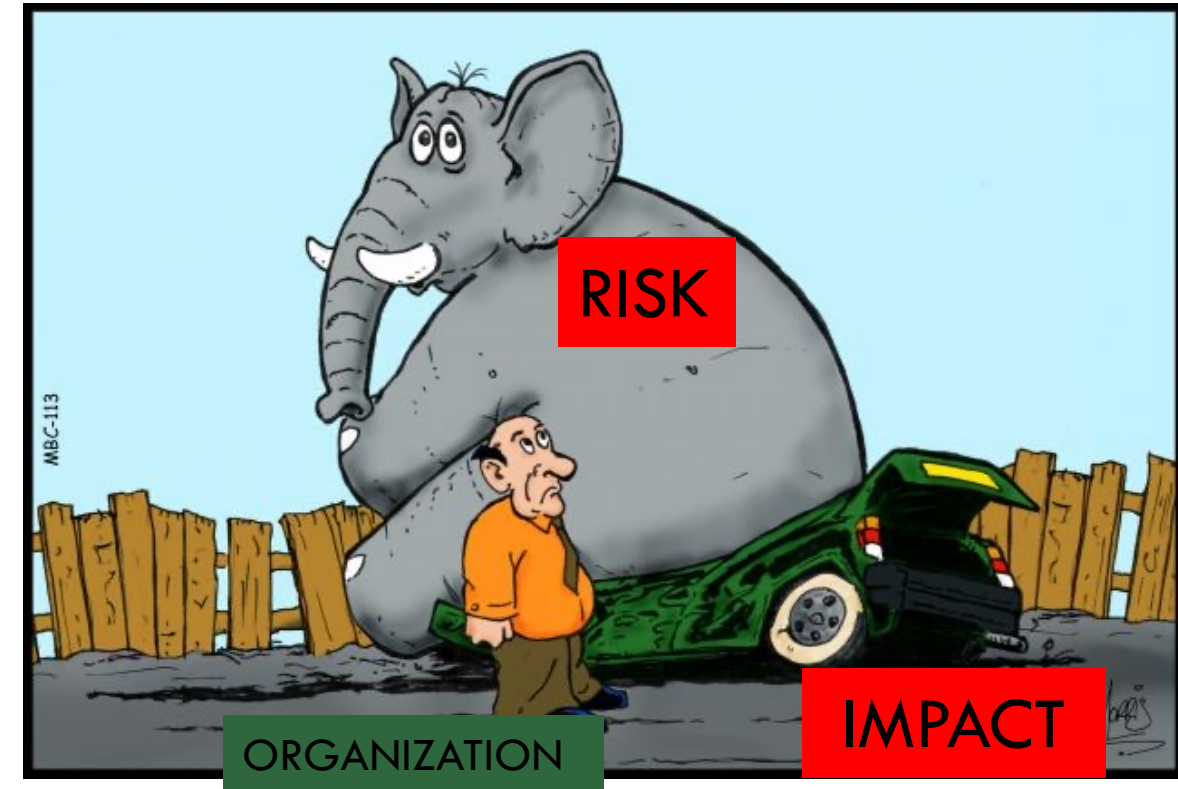
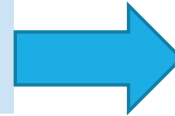


Asset Value

THREAT RATING

Financial
Service
Reputation
Compliance
Average

Threat Rating			
Likelihood		Impact	
Level	Value	Level	Value
Critical	4	Critical	4
High	3	High	3
Medium	2	Medium	2
Low	1	Low	1

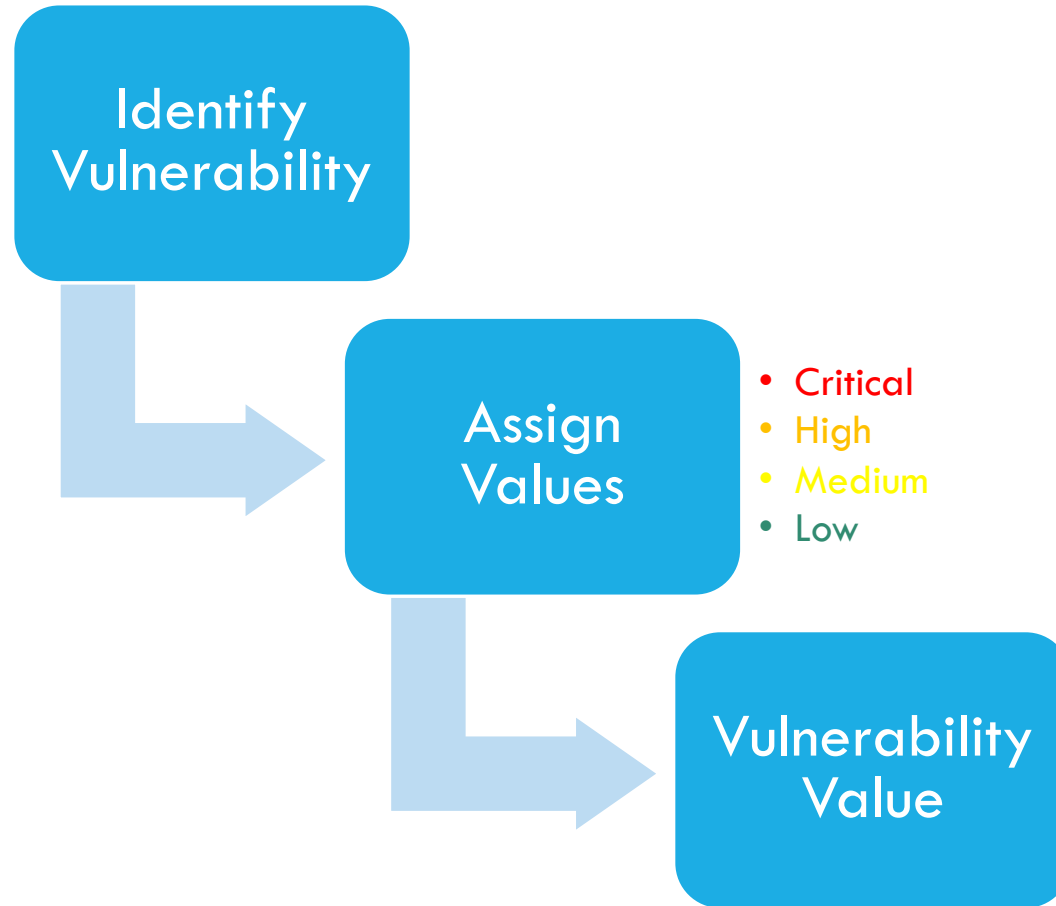


Threat Rating = Likelihood X Impact (Average of four)

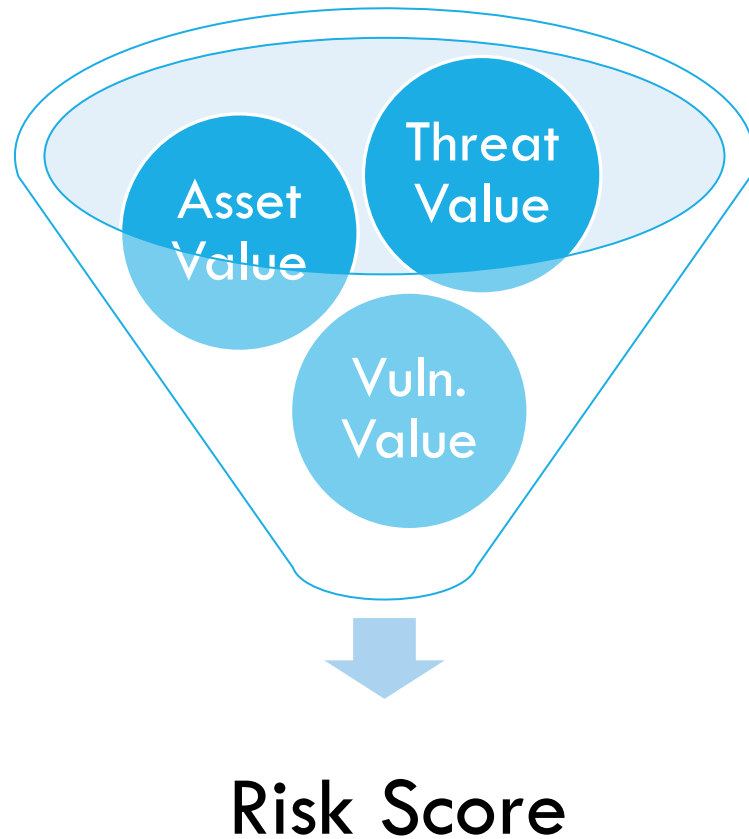
CALCULATING RISK SCORES

INFORMATION ASSETS									
	Threat likelihood		Threat Impact					Threat Level Rating	
	Probability	Value	Financial	Service	Reputation	Compliance	Impact Value	Impact Rating	Threat
Unauthorized access	4	Critical	4	4	4	4	4	Critical	16
Malicious code	3	High	4	4	4	4	4	Critical	12
User Errors	3	High	4	4	4	1	3	High	9
Theft & Fraud	3	High	4	1	4	4	3	High	9
Unauthorized change	1	Low	4	4	4	3	4	Critical	4

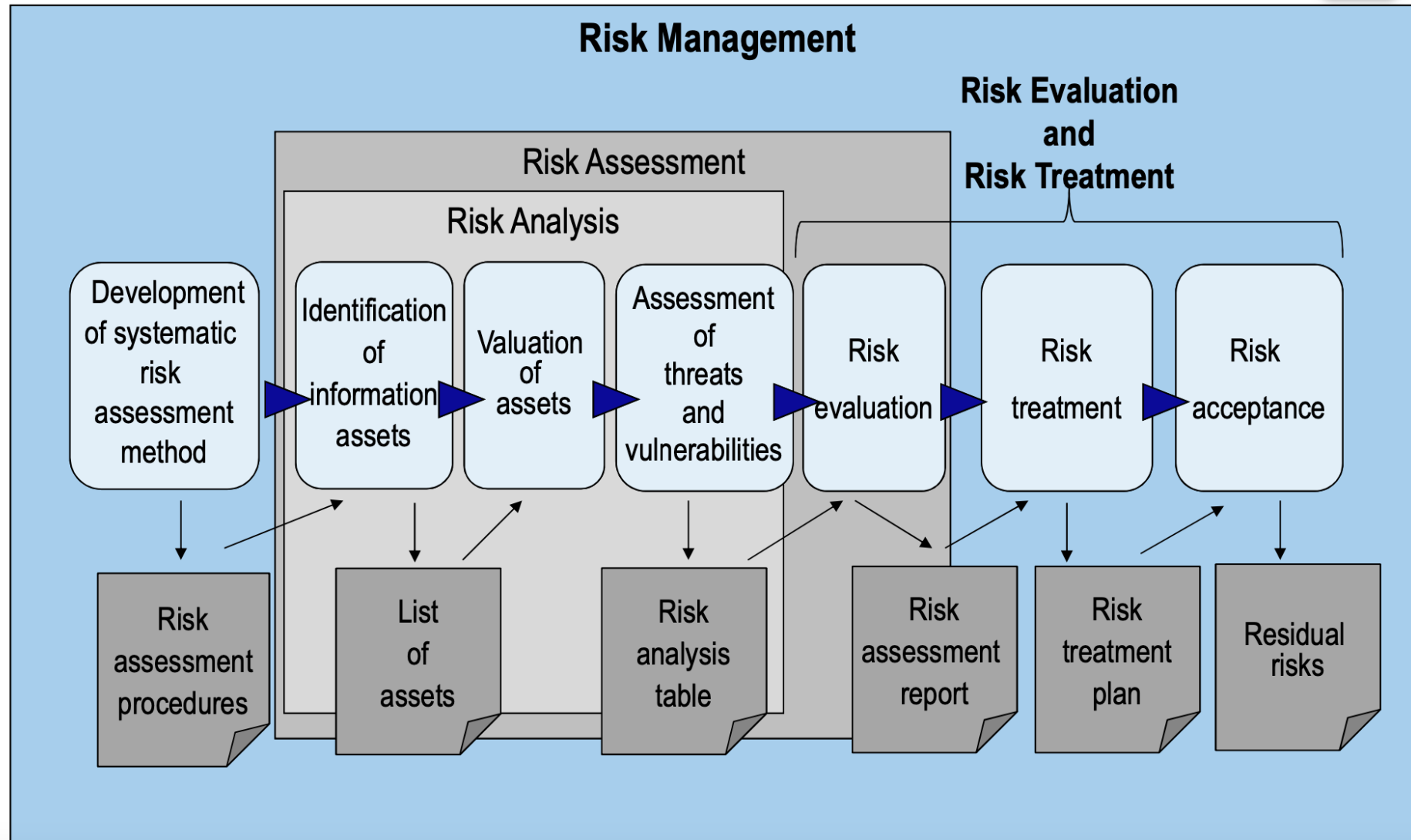
CALCULATING VULNERABILITY VALUE



CALCULATING RISK SCORE



RISK MANAGEMENT

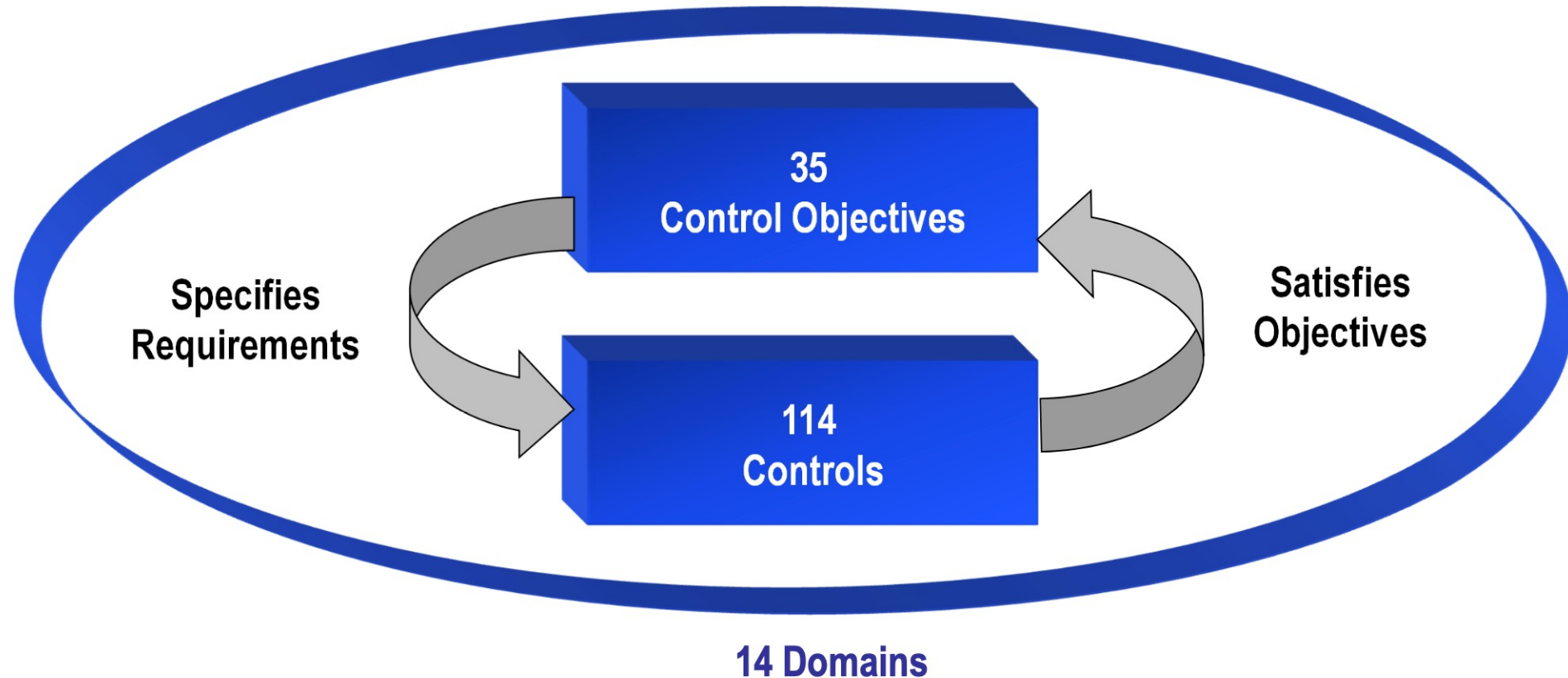


STATEMENT OF APPLICABILITY (SOA)

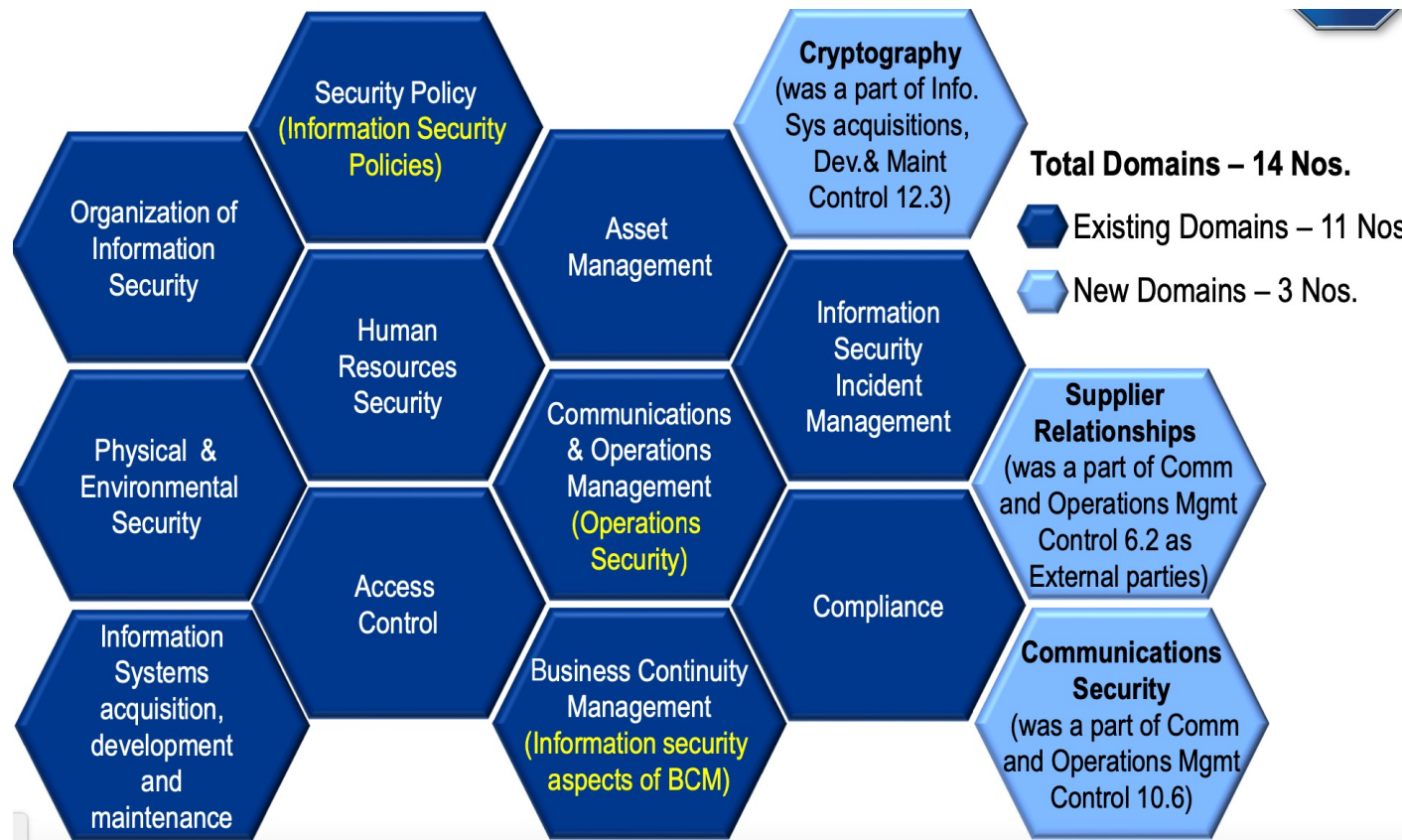
Document describing the control objectives and controls that are relevant and applicable to organization's, based on the results and conclusions of risk assessment and risk treatment process

The Statement will also record the exclusion, with justification, of any controls listed in the ISMS Standard (ISO 27001)

CONTROL OBJECTIVES AND CONTROLS



14 SECURITY DOMAINS OF ISO/IEC 27001



14 SECURITY DOMAINS OF ISO/IEC 27001

A.5 Information Security Policies (1/2) *				
A.6 Organization of Information Security (2/7)*				
A.7 Human Resource Security (3/6)*				
A.8 Asset Management (3/10)*	A.9 Access control (4/14)*	A.10 Cryptography (1/2)*	A.11 Physical and environmental security (2/15)*	A.12 Operations security (7/14)*
A.13 Communications security (2/7)*		A.14 System acquisition development and maintenance (3/13)*		
A.15 Supplier relationships (2/5)*				
A.16 Information security incident management (1/7)*				
A.17 Information security aspects of business continuity management (2/4)*				
A.18 Compliance (2/8)*				

* (control objectives / controls)

A.5.1 Management direction for information security

Control objective:

- To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Controls:

- Policies for information security
- Review of the policies for information security



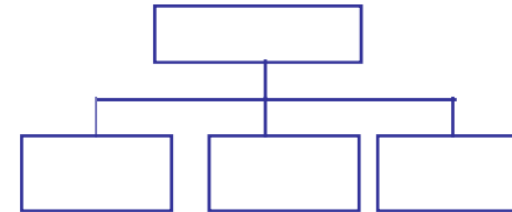
A.6.1 Internal Organization

Control objective:

- To establish a management framework to initiate and control the implementation and operation of information security within the organization.

Controls:

- Information security roles and responsibilities
- Segregation of duties
- Contact with authorities
- Contact with special interest groups
- Information security in project management



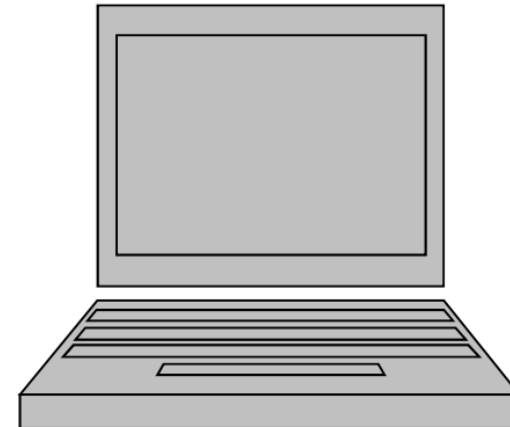
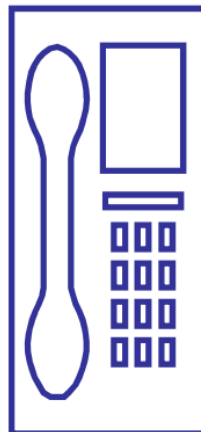
A.6.2 Mobile devices and teleworking

Control objective:

- To ensure the security of teleworking and use of mobile devices.

Controls:

- Mobile device policy
- Teleworking



A.7.1 Prior to employment

Control Objective:

- To ensure that employees and contractors understand their responsibilities and are suitable for the roles they are considered.

Controls:

- Screening
- Terms and conditions of employment

A.7.2 During employment

Control Objective:

- To ensure that employees and contractors are aware of and fulfill their information security responsibilities

Controls:

- Management responsibilities
- Information security awareness, education and training
- Disciplinary process



A.7.3 Termination and change of employment

Control Objective:

- To protect the organization's interests as part of the process of changing or terminating employment.

Controls:

- Termination or change of employment responsibilities

A.8.1 Responsibility for Assets

Control Objective:

- To identify organizational assets and define appropriate protection responsibilities.

Controls:

- Inventory of assets
- Ownership of assets
- Acceptable use of assets
- Return of assets



A.8.2 Information classification

Control Objective:

- To ensure that Information receives an appropriate level of protection in accordance with its importance to the organization.

Controls:

- Classification of information
- Labeling of information
- Handling of assets



Top secret	<input type="checkbox"/>
Secret	<input type="checkbox"/>
Confidential	<input type="checkbox"/>
Restricted	<input type="checkbox"/>
Public	<input type="checkbox"/>

A.8.3 Media handling

Control Objective:

- To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

Controls:

- Management of removable media
- Disposal of media
- Physical media transfer



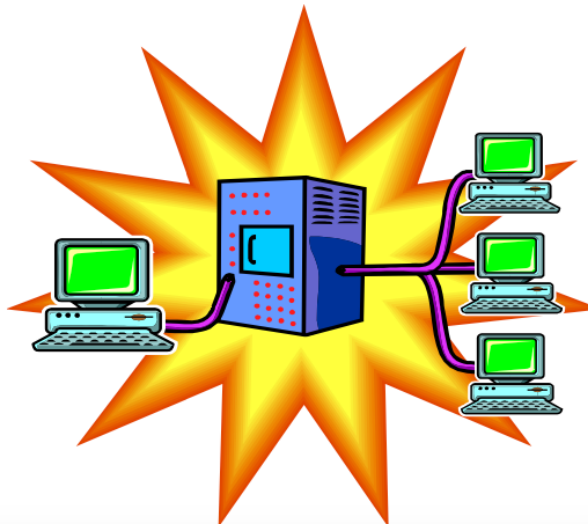
A.9.1 Business requirements of access control

Control Objective:

- To limit access to information and information processing facilities.

Controls:

- Access control policy
- Access to networks and network services



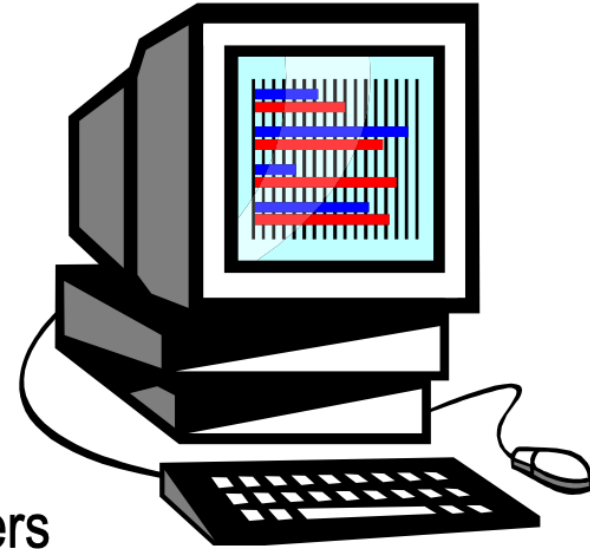
A.9.2 User access management

Control Objective:

- To ensure authorized user access and to prevent unauthorized access to systems and services.

Controls:

- User registration and de-registration.
- User access provisioning
- Management of privileged access rights
- Management of secret authentication information of users
- Review of user access rights
- Removal or adjustment of access rights



A.9.3 User responsibilities

Control Objective:

- To make users accountable for safeguarding their authentication information.

Controls:

- Use of secret authentication information



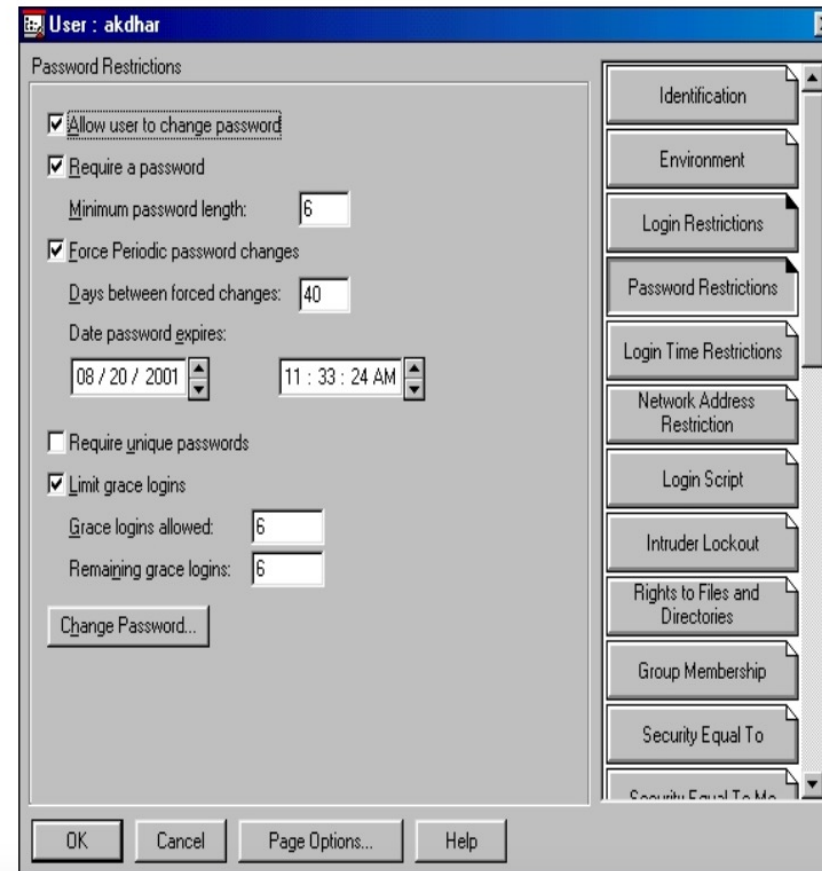
A.9.4 System and application access control

Control Objective:

- To prevent unauthorized access to systems and applications.

Controls:

- Information access restriction
- Secure log-on procedures
- Password management system
- Use of privileged utility programs
- Access control to program source code



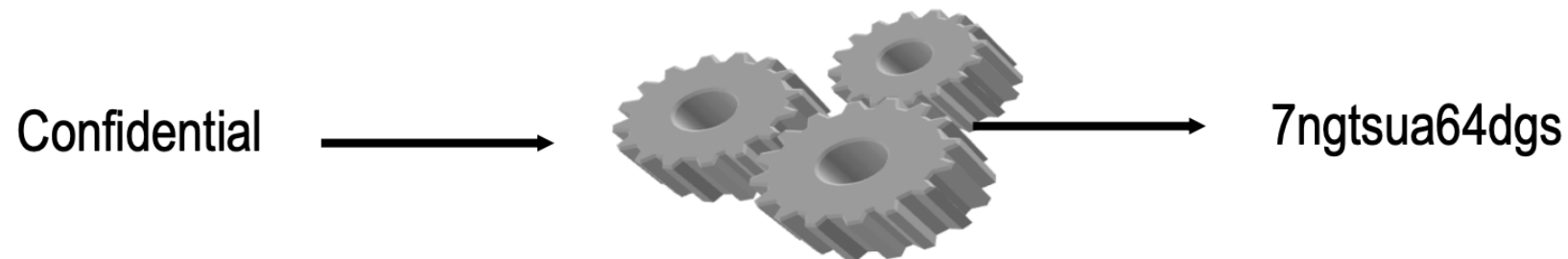
A.10.1 Cryptographic controls

Control Objective:

- To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and / or integrity of information.

Controls:

- Policy on the use of cryptographic controls
- Key management



A.11.1 Secure areas

Control Objective:

- To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

Controls:

- Physical security perimeter
- Physical entry controls
- Securing offices, rooms and facilities
- Protecting against external and environmental threats
- Working in secure areas
- Delivery and loading areas



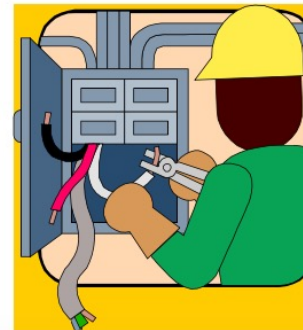
A.11.2 Equipment

Control Objective:

- To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

Controls:

- Equipment siting and protection
- Supporting utilities
- Cabling security
- Equipment maintenance
- Removal of assets
- Security of equipment and assets off-premises
- Secure disposal or re-use of equipment
- Unattended user equipment
- Clear desk and clear screen policy



A.12.1 Operational procedures and responsibilities

Control Objective:

- To ensure the correct and secure operation of information processing facilities.

Controls:

- Documented operating procedures
- Change management
- Capacity management
- Separation of development, testing and operational environments



A.12.2 Protection from malware

Control Objective:

- To ensure that information and information processing facilities are protected against malware.

Controls:

- Controls against malware



A.12.3 Backup

Control Objective:

- To protect against loss of data.

Controls:

- Information backup

A.12.4 Logging and Monitoring

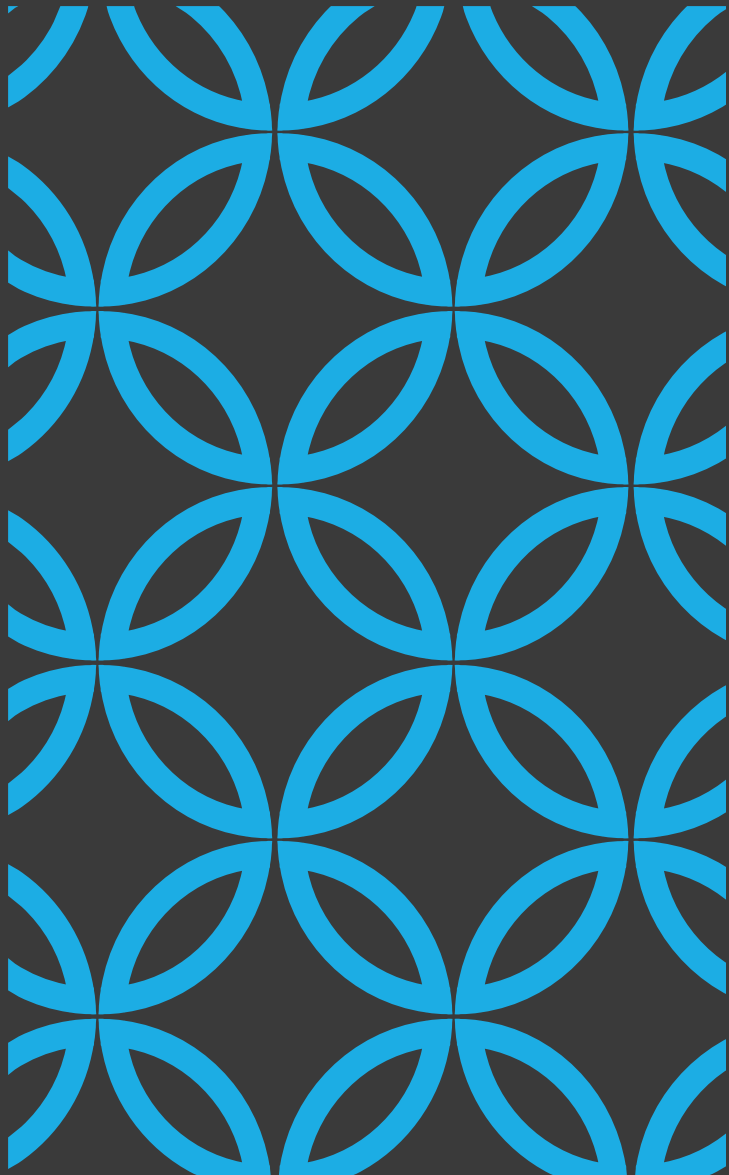
Control Objective:

- To record events and generate evidence.

Controls:

- Event logging
- Protection of log information
- Administrator and operator logs
- Clock synchronization





THANK YOU
