Objectives

After completing this unit, you should be able to:

- Understand the definition of information security
- Understand the key terms and critical concepts of information security
- Understand the Need of Security
- Know what is CIA Triad
- Learn about Threat, Vulnerability and Risk
- Understand Risk Governance & Risk Management
- Know Security Architecture, Governance, Auditing & Compliance
- Understand Security System Design

FTVETI

ICT @ FTVETI

What is an Information System?

Information System (IS): an entire set of

- Software
- Hardware
- Data
- People
- Procedures, Policies, Standards and
- **Networks**

necessary to use information within an organization.

FTVETI

ICT @ FTVETI

Critical Characteristics of Information

The value of information comes from its characteristics:

- **Confidentiality:** privacy/secrecy
- **Integrity:** (Bitwise) identical to the original
- **Availability:** of info, services, etc.
- **Authenticity:** "it is what it claims to be"
- **Accuracy:** free from mistakes and errors
- **Utility:** self-explanatory
- Possession: different from confidentiality

➢ Others:

- **User authentication:** users are who they claim to be
- **Auditability:** there's a record of who accessed what
- **Non-repudiation:** one cannot claim "I didn't sign this"

What is Security?

Definitions:

- **Book:** "The quality or state of being secure- to be free from danger"
- **James Anderson, Inovant:** "Well-informed sense that information risks and controls are in balance"
- **Rita Summers, IBM Systems Journal, 1984:** "Includes concepts, techniques and measures that are used to protect computing systems and the information they maintain against deliberate or accidental threats"

Successful companies should have multiple security "tiers":

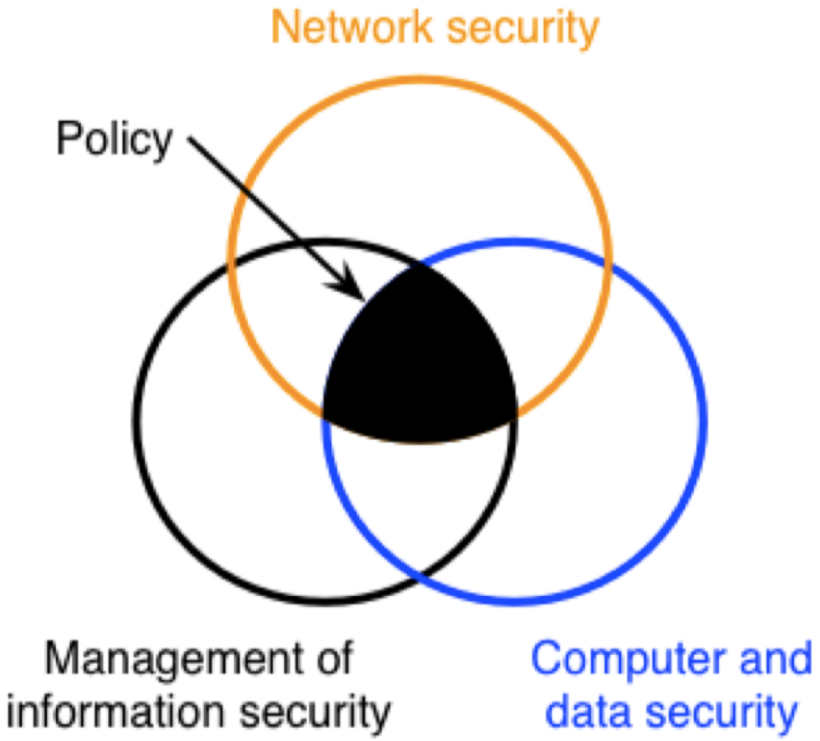
- **Physical security**
- **Personal security**
- **Operations security**
- **Communications security**
- **Network security**
- **Information security**

What is Information Security?

Protection of information and its critical elements, including systems that use, store, and transmit that info

Necessary tools:

- Policy
- Awareness
- Training
- Education
- Technology

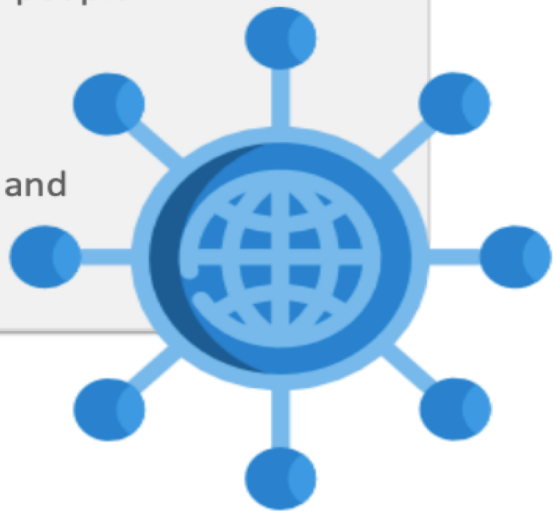


FTVETI

ICT @ FTVETI

Need Of Cyber Security

- We live in an era where internet is used on a daily basis, from net banking to making transactions, we take help of internet
- It is important that the network we are using must be secure so that other people cannot hack our bank details or any personal data
- In order to make the network secure, companies adopt Cyber Security
- Cyber Security is very important as it protects the data from being hacked and misused, it also protects our system from external attacks and so on



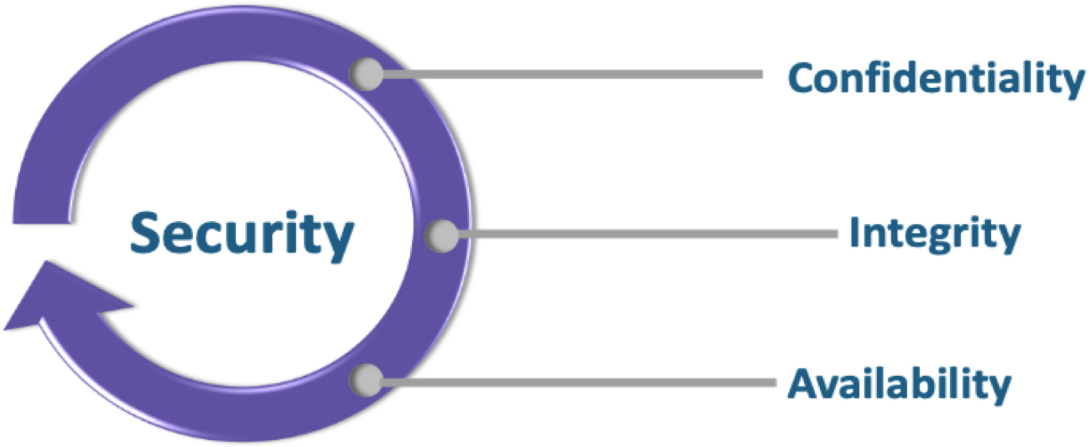
What Is Cyber Security?

Cybersecurity is the combination of **processes**, **practices** and **technologies** designed to protect **networks**, **computers**, **programs**, **data** and **information** from **attack**, **damage** or **unauthorized access**

CIA Triad
Confidentiality | Integrity | Availability

What Is CIA Triad?

- The **CIA Triad** for Information security, provides a baseline standard for evaluating and implementing information security – irrespective of the system and/or organization in question
- CIA Triad have three core pillars, each having their individual requirements and processes, they are:



C – I – A

- Data or an information system is accessed by only an authorized person
- User Id's and passwords, access control lists (ACL) and policy based security represents confidentiality

Confidentiality

- Data is edited by only authorized persons and remains in its original state when at rest
- Data encryption and hashing algorithms are key processes in providing integrity

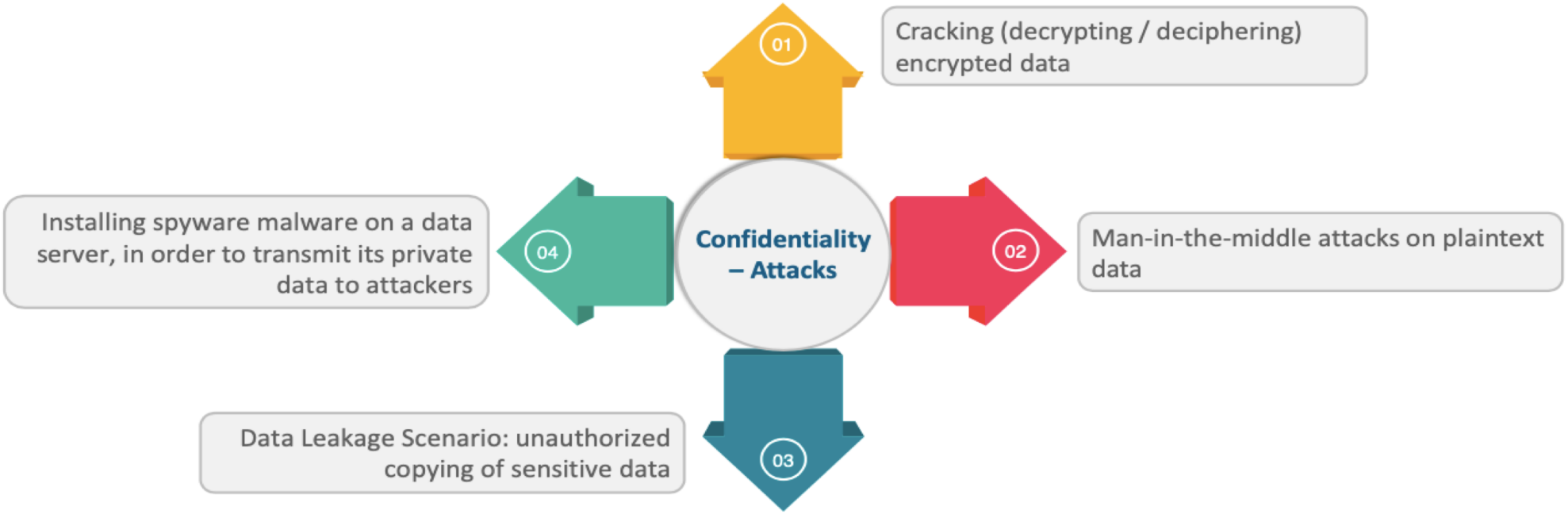
Integrity

- Data & information systems are available when required to apt entities
- Backups, load balancing, DDOS Protection, software patching/upgrading and network optimization ensures availability

Availability

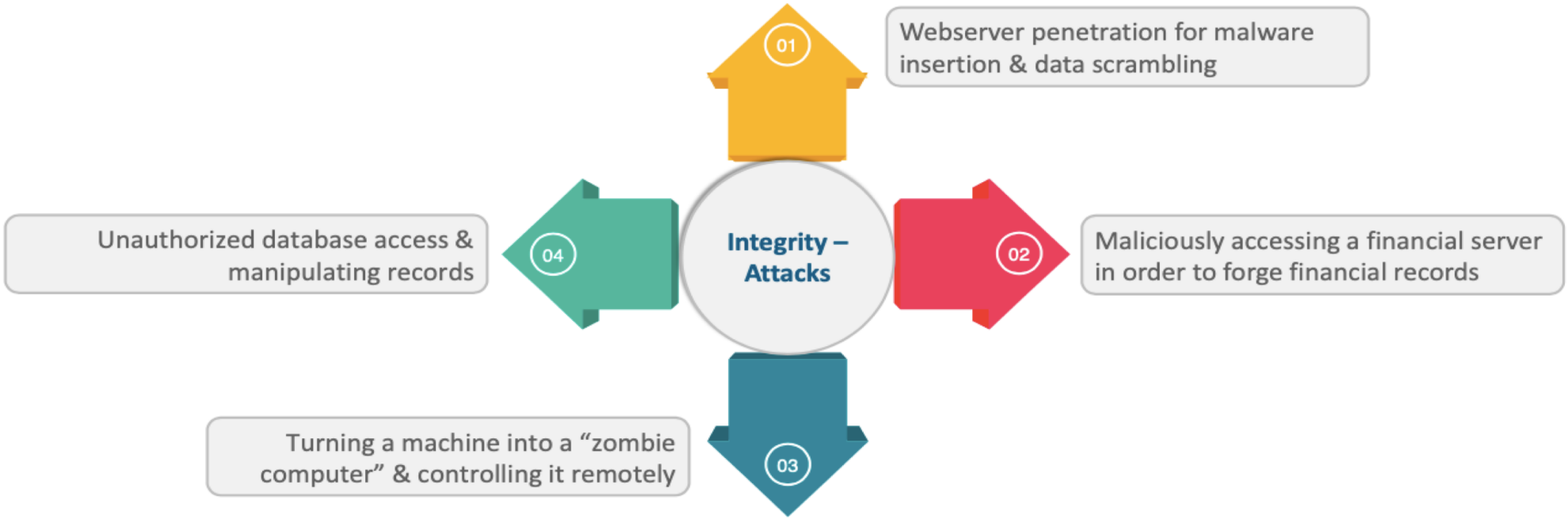
Confidentiality

Confidentiality is all about making sure that data is accessible only to its intended (authorized) individual



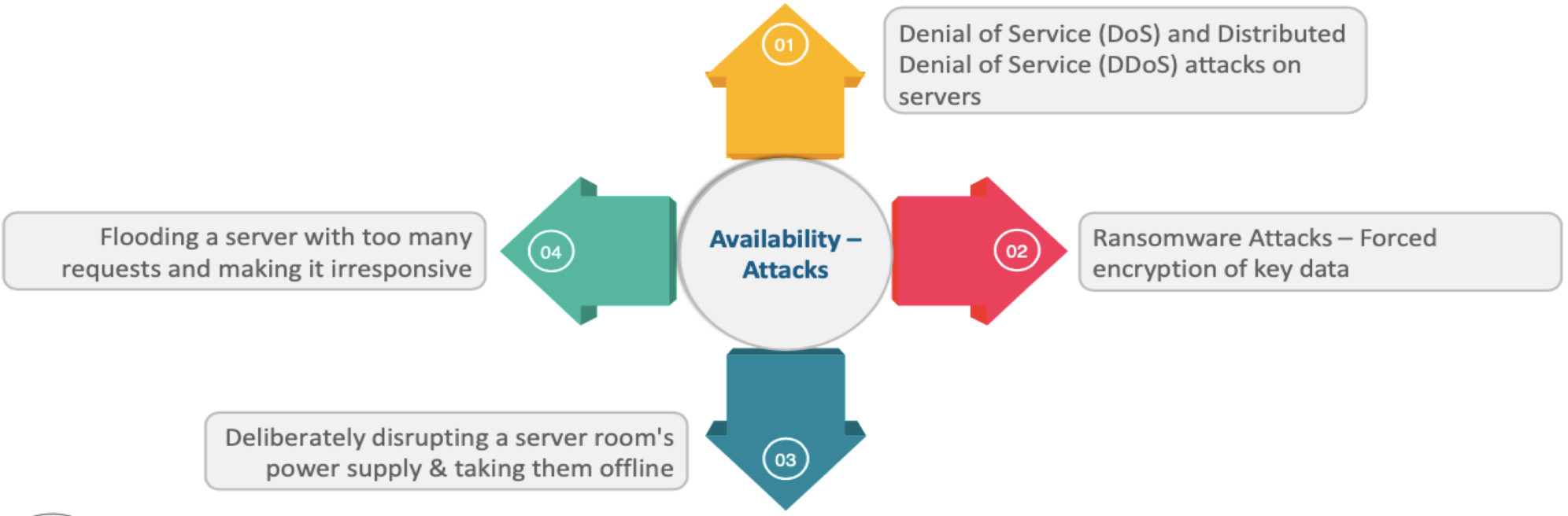
Integrity

Integrity is all about making sure that data is kept properly intact without it being meddled with in an unauthorized way



Availability

Availability is all about making sure that data and computers are available as needed by authorized parties



Bits To Ponder

All cyber attacks have the potential to threaten one or more of the three elements of the CIA triad. The model is significant because it can help security practitioners with risk assessment, asset management, and designing security measures

Domain of Information Security involves multiple interrelated & complex topics and the concept of CIA triad helps bringing some clarity of thought to security practitioners to assess, prioritize and evaluate the assets (target elements) to be protected and the protection measures as well

Threat, Vulnerability And Risk


Let us first understand what is **Threat** and different **Threat Assessment Techniques** in case of Cyber Security

Threat

Threat refers to someone with the potential to do harm to a system or an organization

Natural Threats

- Earthquakes, floods or tornados

Unintentional Threats

- Inadvertent errors by employees causing deletion or publication of private data

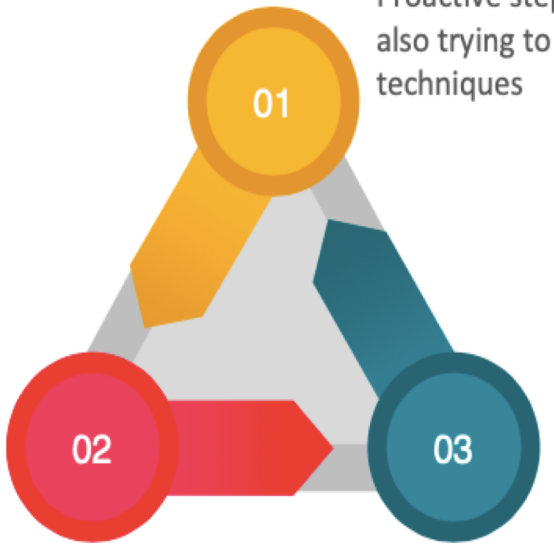
Intentional Threats

- Spyware, malware (worms, virus, ransomwares)
- Malicious actions by a disgruntled employee

Threat Assessment Techniques

VAPT (Vulnerability Assessment & Penetration Testing)

Proactive step to periodically determine known open vulnerabilities and also trying to break into a given system using available tools & techniques

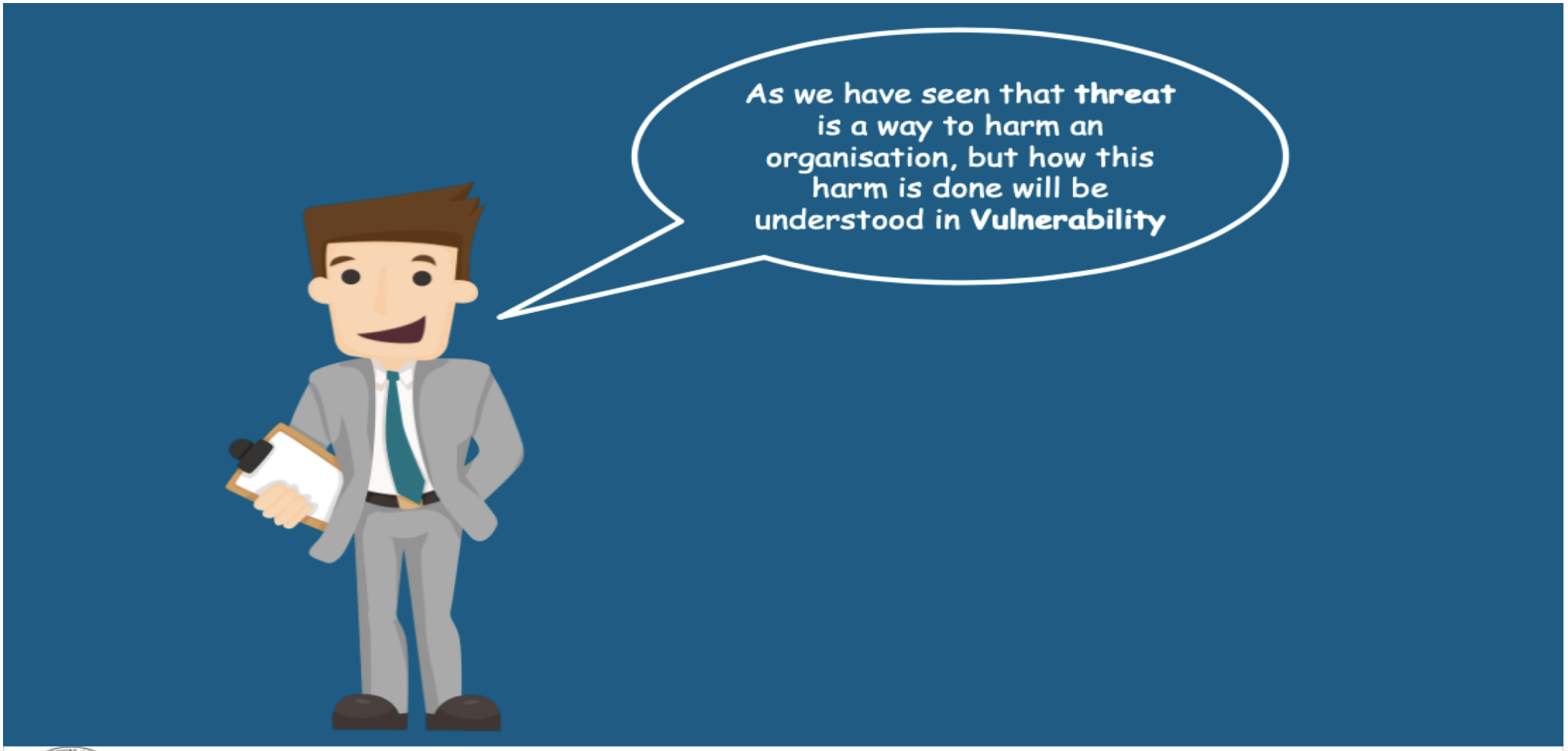


RCA (Root Cause Analysis)

Despite all the controls, Incidents do occur & RCA techniques help an organization to dig deeper into the cause of incidents and hence pave the way to fix the gaps to avoid future similar damage

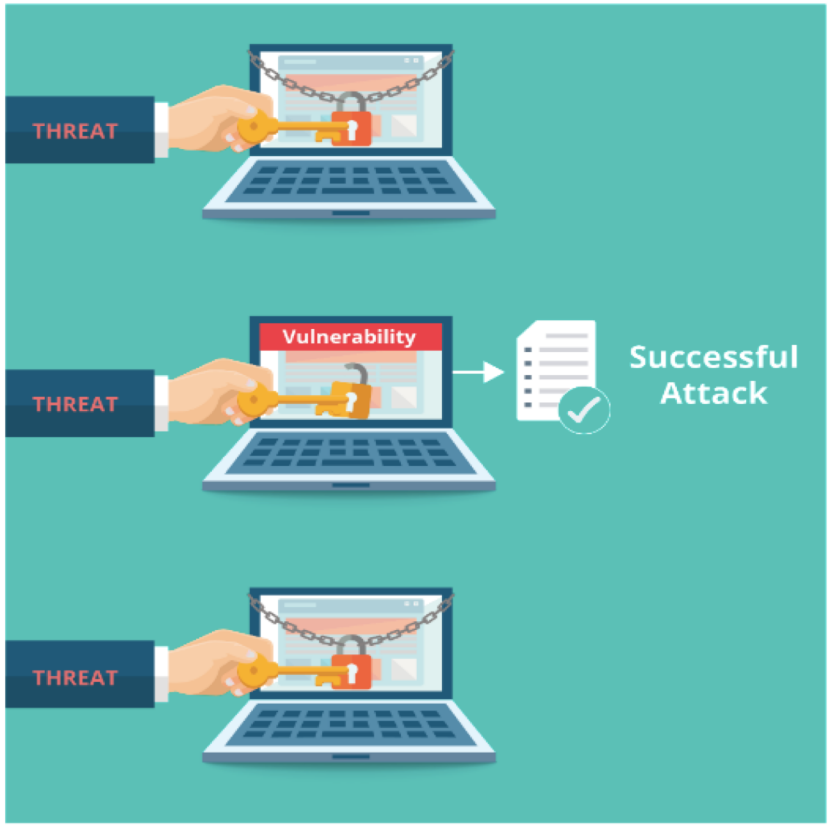
Threat Intelligence

Continual way of gathering Threat specific data, knowledge about potential threat actors, **TTPs** (Tactics, Techniques & Procedures) and **IOCs** (Indicators Of Compromise) that can affect a given organization so as to immunize it before the potential attack to either rapidly & timely catch a perpetrator or minimize the potential impact


As we have seen that **threat** is a way to harm an organisation, but how this harm is done will be understood in **Vulnerability**

Vulnerability

- **Vulnerability** refers to a weakness of an asset (resource) that can be exploited by one or more attackers(threat actors). In other words, it is an issue or bug that allows an attack to be successful
- In context of cyber world, an open vulnerability refers to a known or an unknown bug/ defect in hardware or software which remains to be fixed and is prone to be exploited to cause a damage to one of the elements within CIA triad

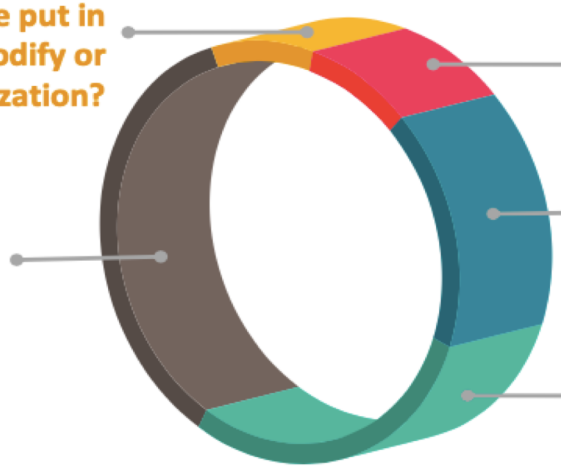


Understanding Vulnerability

- Testing for open vulnerabilities is critical to ensuring continued security of systems. This is achieved by identifying weak points and developing a strategy to respond timely
- Here are some questions to ask when determining your security vulnerabilities:

What kind of network security measures are put in place, to determine who can access, modify or delete information from within your organization?

Is the key data backed up and stored in an accessible and secure off-site location?



Is the key data stored in the cloud? If yes, how exactly is it being protected from cloud vulnerabilities?

What kind of anti malware defence is in place? Are the licenses valid & current? Is it running as frequently as expected?

Is data recovery plan defined and tested, to be used in an event of a vulnerability being exploited?

- **Understanding vulnerabilities is a key step towards managing risk !**

Vulnerability Scoring

One of the most famous and used vulnerability scoring model is given by First, & is known as CVSS

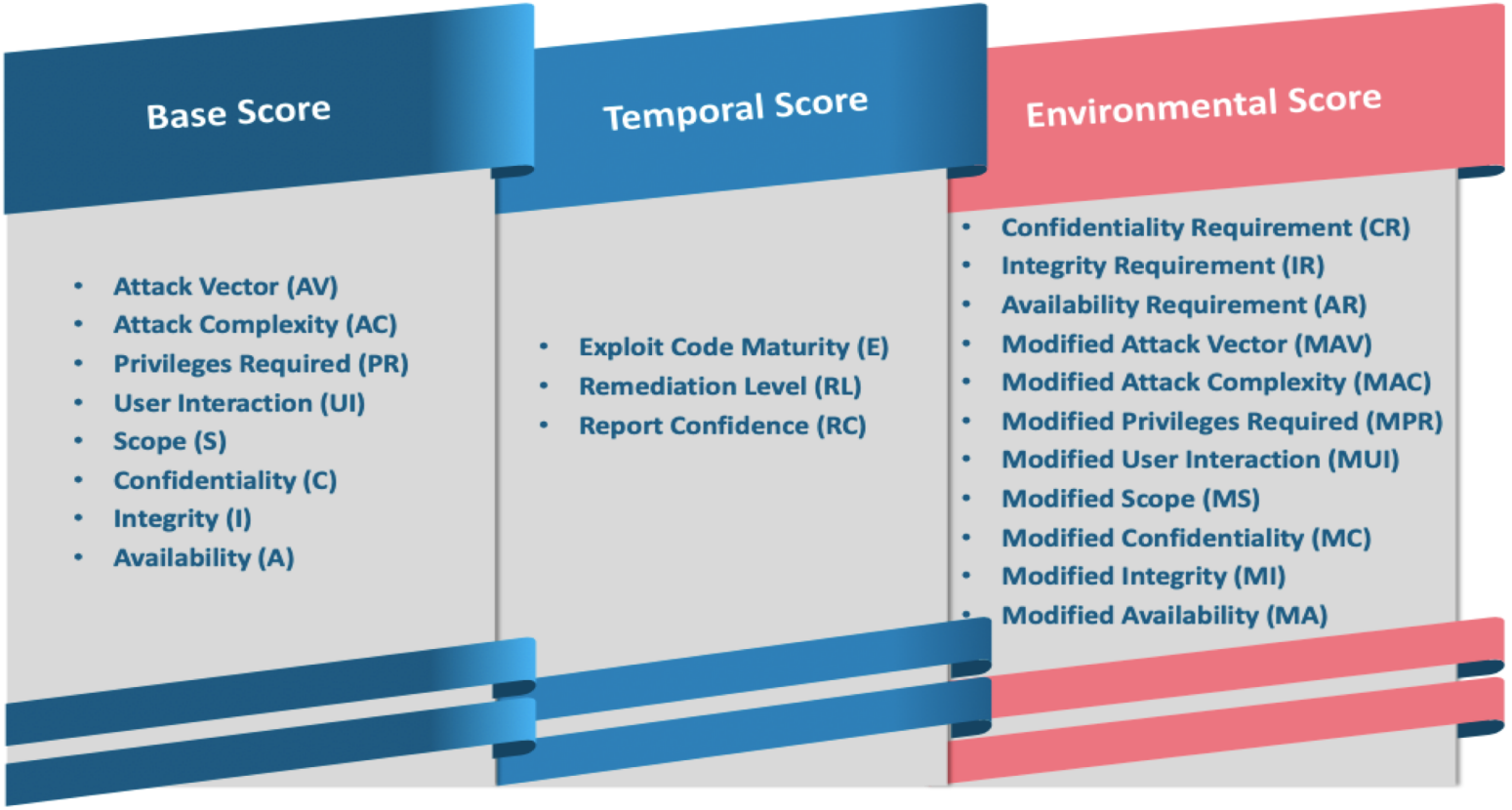
The **Common Vulnerability Scoring System (CVSS)** is a way to capture the principal characteristics of a vulnerability and produce a numerical score in order to reflecting its severity

This numerical score can then be translated into a qualitative representation (such as low, medium, high or critical) to help organizations properly assess and prioritize their vulnerability management processes

CVSS is a published standard used by organizations worldwide

Tip : *Try out the Latest CVSS Calculator. It is available at https://www.first.org/cvss/calculator/3.0*

CVSS Scoring Parameters



We have seen how Threat n Vulnerability can harm our system. Combination of both decides the **Risk** for a system as shown below:

*Risk = Threat * Vulnerability*

*Risk = Impact (of the vulnerability getting exploited) * Frequency*

What Is Risk?

- Risk refers to the potential for loss or damage when a threat exploits a vulnerability
- Examples include the following:

Financial losses as a result of business disruption

Loss of privacy

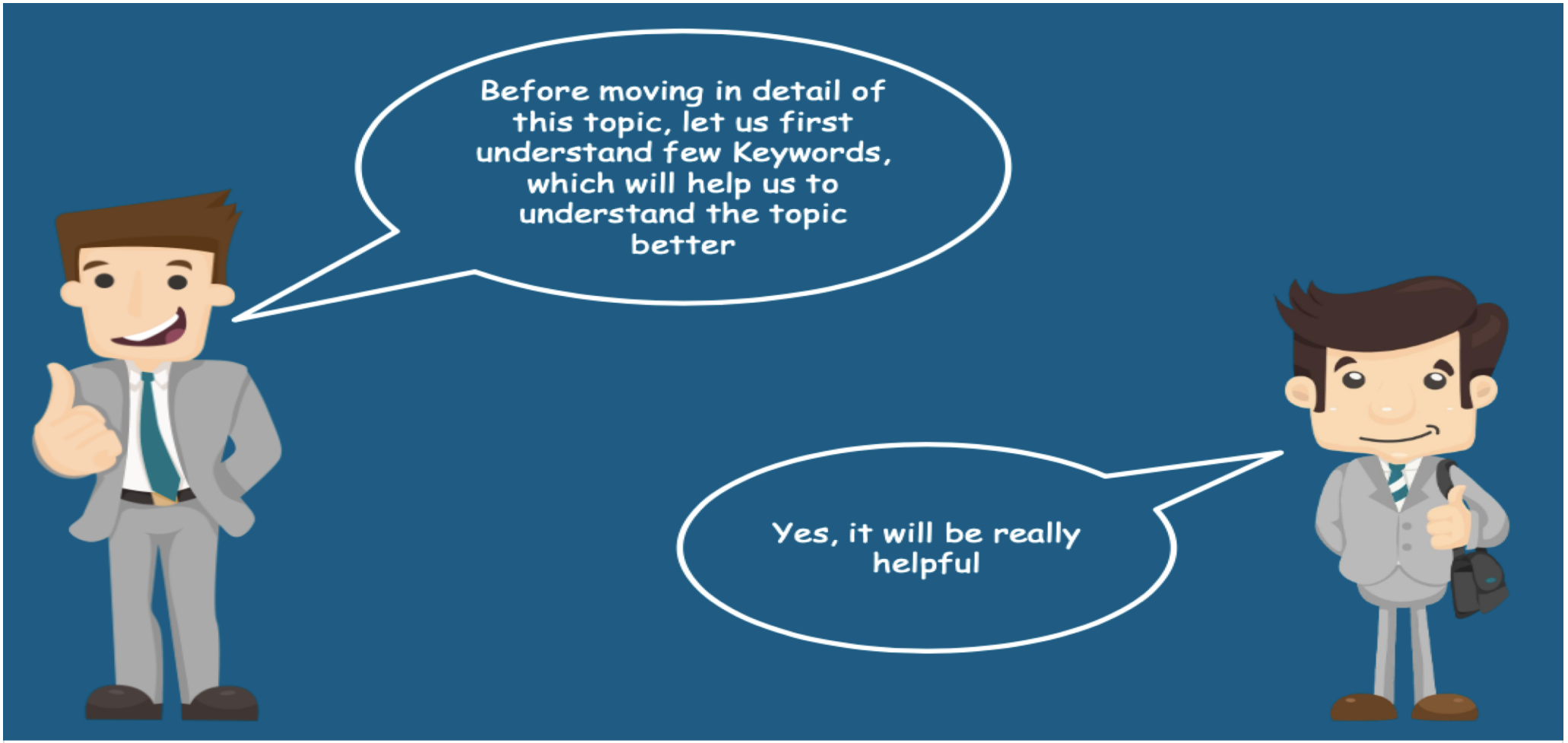
Reputational damage

Legal implications

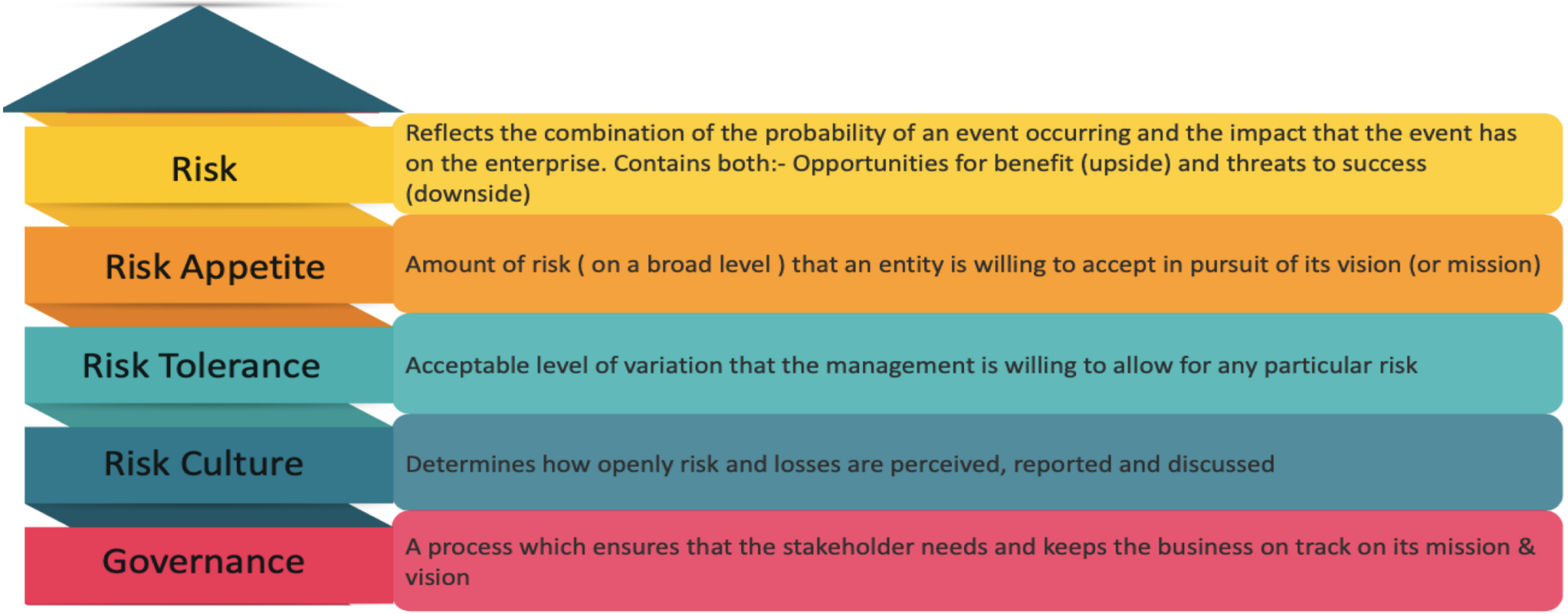
Even include loss of life

Key Considerations For Risk Management Strategy

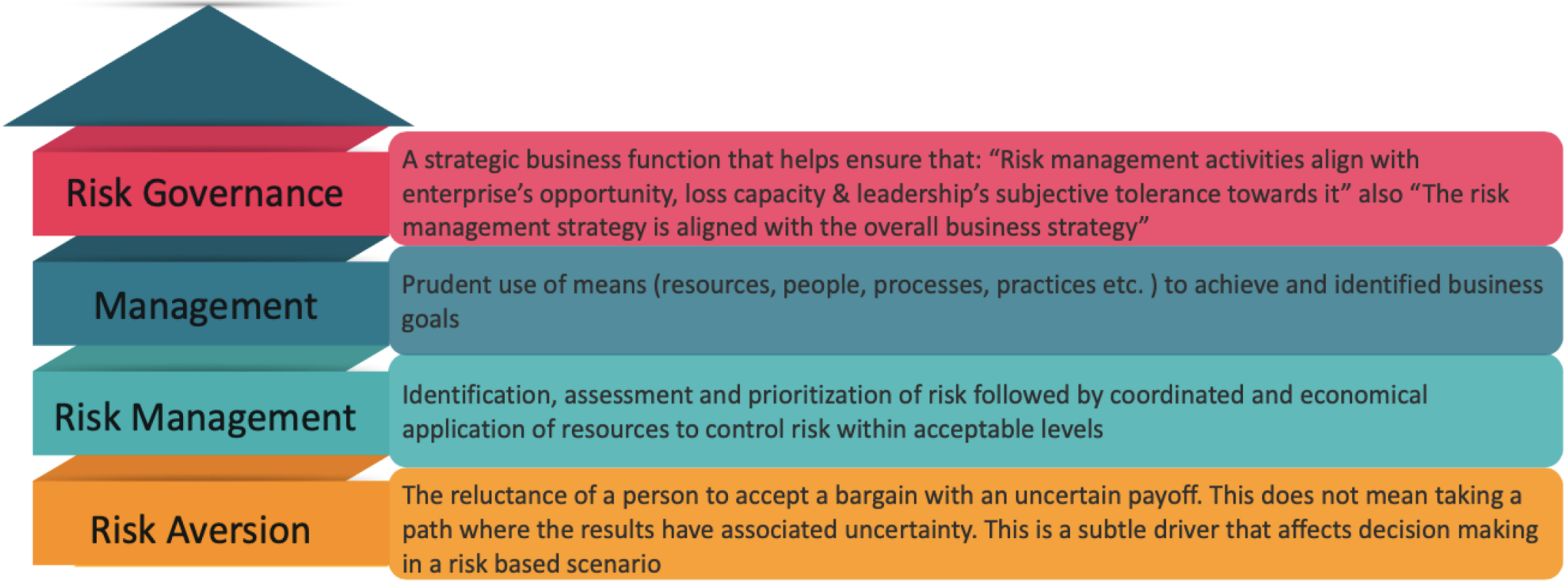
Risk Governance & Risk Management


Before moving in detail of this topic, let us first understand few Keywords, which will help us to understand the topic better
Yes, it will be really helpful

Top View For Risk Governance & Management



Top View For Risk Governance & Management

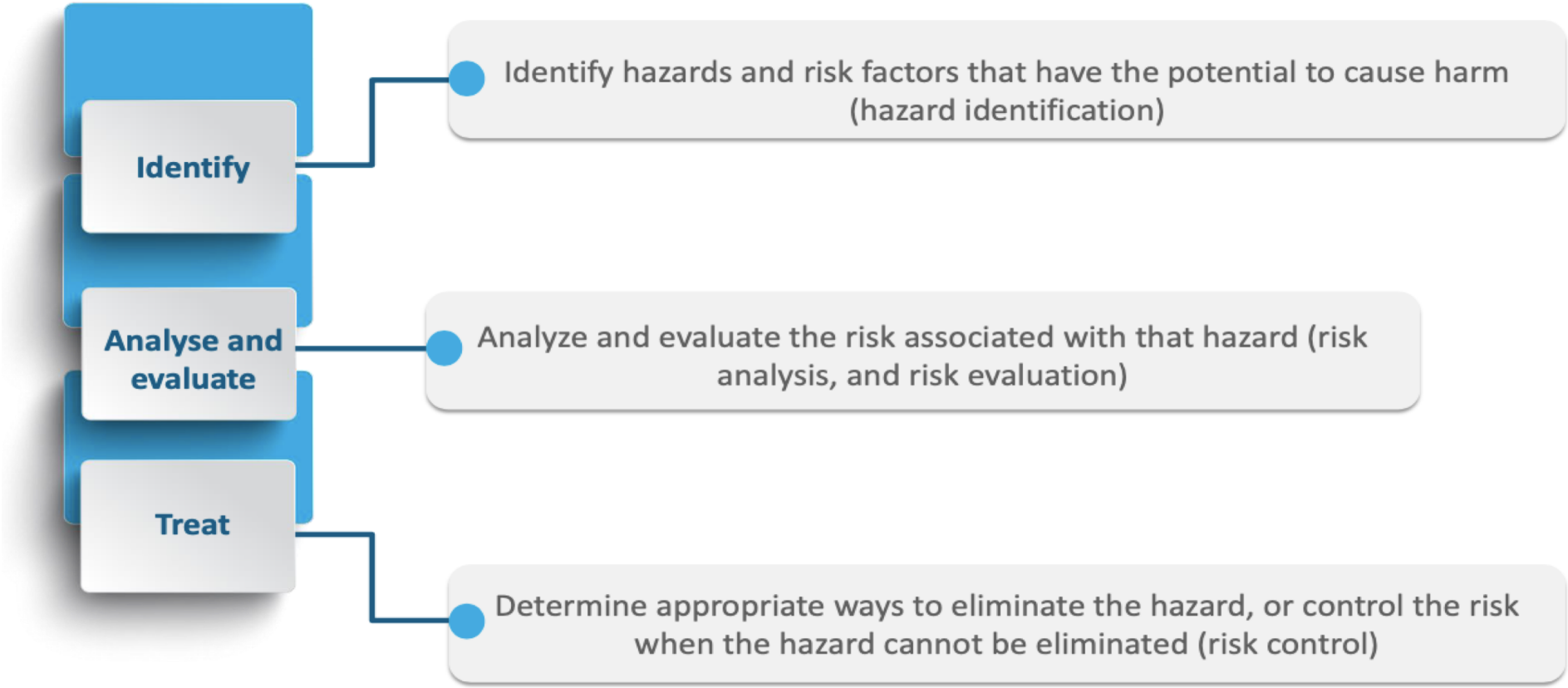



We know how to govern and manage Risk. But, we should also know the effort which is used to understand the risks faced by an organization and this begins with Risk Assessment

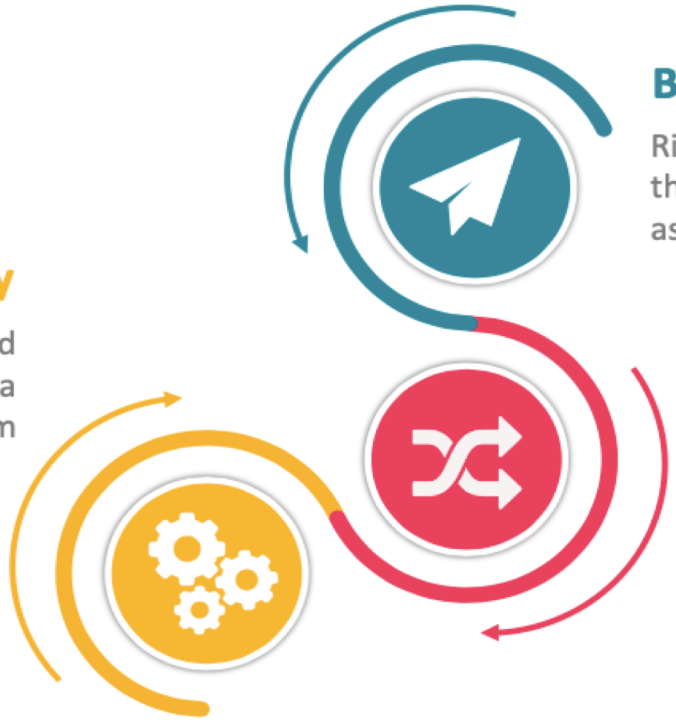
What Is Risk Assessment?

- Risk is the probability that a threat actor (cause) will exploit a vulnerability (weakness) in the system and thereby create an effect unfavorable to the system. Hence understanding the risks facing an organization is paramount before formulating an appropriate response for addressing those risks
- The effort to understand the risks faced by an organization, begins with **Risk Assessment**

Risk Assessment



When To Perform Risk Assessment?



Beginning

Risk Assessment should be performed for the first time at the beginning of the project lifecycle to evaluate risks associated with the activity

Periodically

Finally , a risk assessment should occur periodically as a part of a reassessment program

Change(s)

Further Risk assessment should occur as a part of the change management process. Both changes initiated by the organization and changes in the threat landscape should initiate a risk assessment


After Assessment we need to Analyse the Risk too

Risk Analysis

- Information Security **Risk Analysis** begins by selecting an approach to evaluate the risks facing an organization
- The two most common approaches for conducting risk analysis include:

Quantitative Risk Analysis

Qualitative Risk Analysis

Quantitative Risk Analysis

- Focuses on mapping the probability of occurrence of a specific event to the expected cost associated with the event
- General Formula:
  - **ALE = ARO x SLE**
    - **ALE** = Annualized Loss Expectancy
    - **ARO** = Annualized Rate of Occurrence
    - **SLE** = Single Loss Expectancy
- Quantitative method is more accurate but also demands a clarity and accuracy on inputs. Unreliable or inaccurate data affects the outcome of the decision making process. Probability can rarely be precise and, in some cases, can promote complacency

Qualitative Risk Analysis

- Focuses on mapping the perceived impact of a specific event occurring to a risk rating agreed upon by the organization
- This subjective analysis approach is less precise than the quantitative approach
- Allows flexibility to define risk according to categories like low, medium, high / green, amber, red and so on
- As per ISO 27005, qualitative risk analysis is appropriate in the following situations:
  - As an initial screening activity to identify risks that require more detailed analysis.
  - Where this kind of analysis is appropriate for decisions
  - Where the numerical data or resources are inadequate for a quantitative risk analysis


Risk treatment is the next step once we have assessed and analysed the Risk

Risk Treatment

- Risk Treatment is a process to modify risk
- Information security Risk treatment involves taking measures to address either the impact or probability of occurrence thereby reducing the overall risk exposure of an organization
- Risk Treatment is a business decision. The **CISO** (Chief Information Security Officer) supports the decision-making process by identifying risks & recommending treatment options. Ultimately, the business owner must choose the treatment option that addresses the risk concern most effectively, to support the organization's goals
- CISO may offer support related to risk treatment, but the final decision belongs to the business
- **Points to ponder :**
  - **Inherent Risk** : Risk that comes with the very nature of the business
  - **Residual Risk** : Risk that remains after application of controls

Risk Treatment Options

- Organizations have **FOUR** options to support their risk treatment strategy
- The term used to describe the strategy depends upon the chosen framework to support risk management. Example: NIST, ISO & RISK-IT framework use different terms in their discussion of risk treatment, but the terms produce similar consequences
- **Risk Treatment Options are:**
  - Risk Acceptance or Retention
  - Risk Avoidance or Elimination
  - Risk Sharing or Transfer
  - Risk Modification or Mitigation

Risk Acceptance Or Retention

- **Risk Acceptance or Retention**
- Risk Avoidance or Elimination
- Risk Sharing or Transfer
- Risk Modification or Mitigation

- When an organization acknowledges a risk, and chooses deliberately to operate without applying any one of the other treatment options
- In many cases, even after applying other risk treatment options there remains a risk known as "residual risk" which has to be accepted in order to operate further
- **Risk Acceptance** is associated with opportunities and are integral aspect of business to continue
- Ideally residual risk within the thresholds of acceptable limits (risk appetite) of the business is formally accepted and such decisions map to the commitment of the top management towards the vision or mission of the organization

Risk Avoidance Or Elimination

- Risk Acceptance or Retention
- **Risk Avoidance or Elimination**
- Risk Sharing or Transfer
- Risk Modification or Mitigation

- When an organization chooses to completely avoid the cause of the risk & not operate in order to remove the risk & eliminate its effect on the activity all together
- At times when **Risk Assessment** shows that the damage could perhaps be of a great loss even after considering other risk treatment options, organizations tend to avoid taking such risks & hence either change the business plan or the specific activity which may lead to such identified risk
- Compliance Risks, Risks from natural disasters or Risks from physical threats/warfare are typical to go for such an option

Risk Sharing Or Transfer

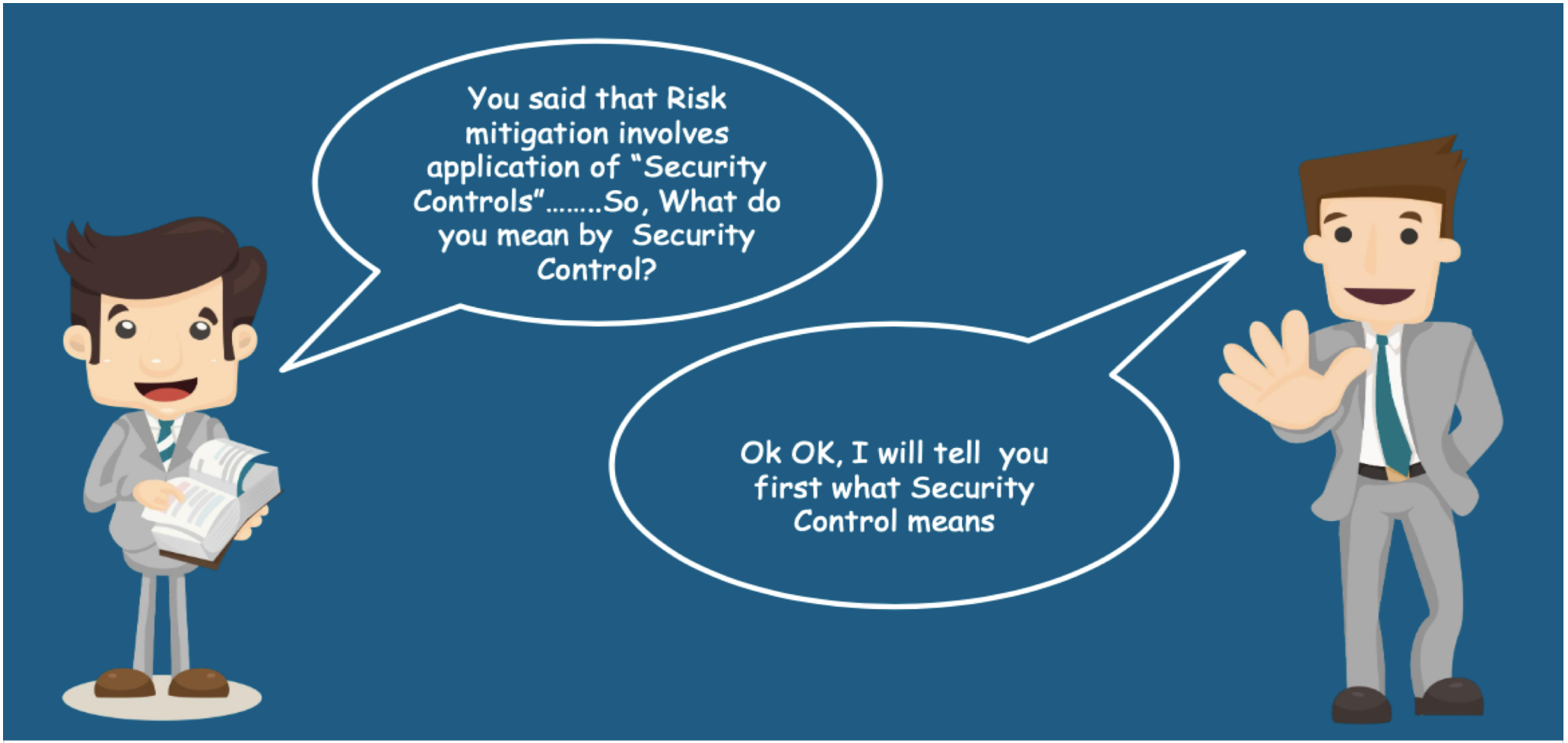
- Risk Acceptance or Retention
- Risk Avoidance or Elimination
- **Risk Sharing or Transfer**
- Risk Modification or Mitigation

- **Risk Sharing** relates to reassigning accountability for a risk to another entity or organization
- Most often this is accomplished by purchasing insurance that will reduce the direct costs of a covered event or reduce the cost of remediation
- Although shared or transferred risk can reduce costs associated with risk management, an organization cannot transfer risk entirely to another organization. The organization ultimately owns the risk, and shares the cost of potential outcomes.
- Insurance involves premium which is a direct function of the risk profile of the organization willing to insure its assets

Risk Modification Or Mitigation

- Risk Acceptance or Retention
- Risk Avoidance or Elimination
- Risk Sharing or Transfer
- **Risk Modification or Mitigation**

- **Risk Modification** is the most common risk treatment option. An organization seeks to change risk exposures or outcomes by applying security controls to a process, system, or environment when they are performing risk modification
- Some risk management frameworks describe modification in terms of mitigation – the extent to which the severity of the risk has been reduced
- Risk mitigation involves application of "Security Controls"


You said that Risk mitigation involves application of "Security Controls".....So, What do you mean by Security Control?
Ok OK, I will tell you first what Security Control means

Security Control

- A **Control** is a measure/ safeguard/ countermeasure that is used to modify the risk
- **Information Security Controls** include any process, policy, procedure, guideline, practice or organizational structure and can be administrative, technical, managerial or legal in nature that modifies the Information Security Risk

Security Control Types

Types Of Controls By Actions

Preventive Controls

Such controls proactively prevent a risk from being manifested

For ex: System Hardening, SOD (Segregation Of Duties) and so on

Detective Controls

Detective controls identify the existence of anomalous or improper activity

For ex: IDS (Intrusion Detection Systems), reconciliation, integrity hash check and many more

Corrective Controls

Corrective controls modify an environment & take action to restore the environment to its normal operating state

For ex: IPS (Intrusion prevention systems), Corrective IdAM controls (anomalous access revoke) and many more

Deterrent Controls

Deterrent controls discourage the exploitation of a vulnerability or system

For ex: Login banners, system-use notifications and so on

Control Selection

Controls usually come with an associated cost, therefore selection of controls with optimal cost-benefit is the key. The expenditure associated with a control include acquisition, implementation, maintenance, operational support, & monitoring costs. Organizations assess these costs by evaluating the desired level of risk mitigation and the value of the asset to be protected

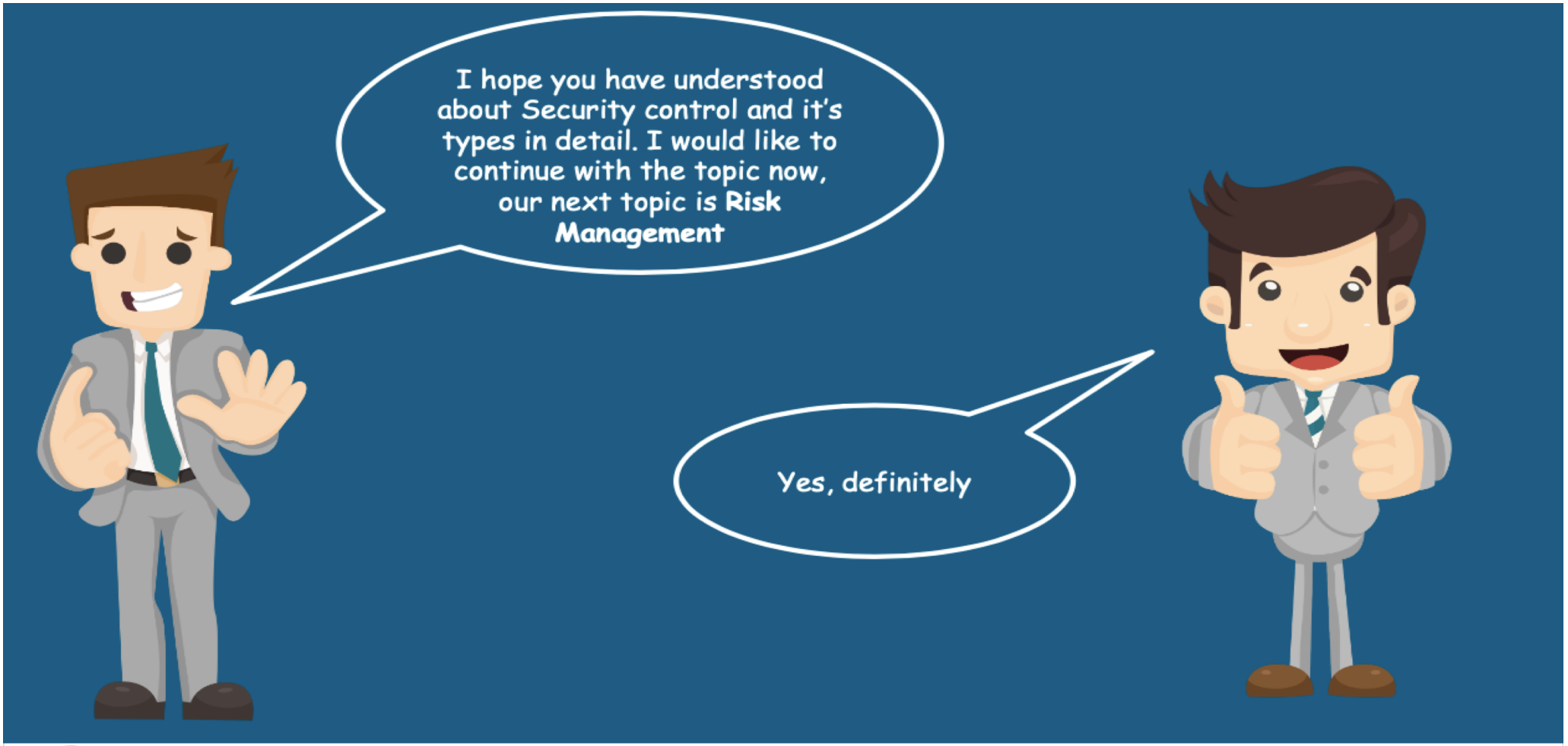
Control Selection – Methods

The following methods are useful for control selection in practice :

- **Industry best practices / benchmarks and standard control catalogs (ISO 27002 , NIST SP 800-53)**
- **Systematic assessment & evaluation of unique risks facing the organization**

1. **Key Controls :** Key controls are a set of indispensable controls, that mitigates significant risk to the organization. Failure of such key controls could be catastrophic if exploited

2. **Compensating Controls :** Compensating controls provide alternative approach to achieve the intended outcome of a desired primary control. Such controls are considered usually when the primary recommended control is too expensive / impractical or difficult to realize


I hope you have understood about Security control and it's types in detail. I would like to continue with the topic now, our next topic is **Risk Management**
Yes, definitely

Risk Management

Risk Management is the identification, assessment and prioritization of risk followed by coordinated and economical application of resources to minimize, monitor & control the probability and/or impact of adverse events or to maximize the realization of opportunities

Essentials Of Risk Management


We will now move on to the Risk Management Framework, which will give us a clear idea about Managing Risk

RMF: Risk Management Frameworks

ICT @ FTVETI

NIST Risk Management Framework Overview

The selection and specification of security controls for a system is accomplished as part of an organization-wide information security program that involves the *"Management Of Organizational Risk"* – that is, the risk to the organization or to individuals associated with the operation of a system

The management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for a system---the security controls necessary to protect individuals and the operations and assets of the organization

NIST Risk Management Framework (SP 800-37)

The **NIST Risk Management Framework (SP 800-37)** provides a process that integrates security and risk management activities into the system development life cycle. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations

The activities (as shown in image) related to managing organizational risk are paramount to an effective information security program and can be applied to both new and legacy systems within the context of the system development life cycle and the Federal Enterprise Architecture

Risk Management – Steps

Assess

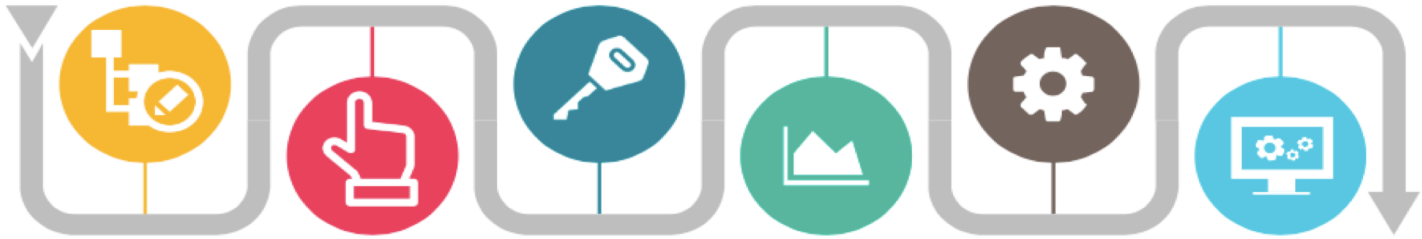
Assess security control using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, & producing the desired outcome so as to meet the security requirements

Select

Selects an initial set of baseline security controls for the system based on the security categorization

Monitor

Monitor and assess selected security controls in the system on an ongoing basis , & reporting to appropriate levels



Categorize

Categorize the system and the information processed, stored, and transmitted by that system based on an impact analysis

Implement

Implement the security controls and document how the controls are deployed within the system and environment of operation

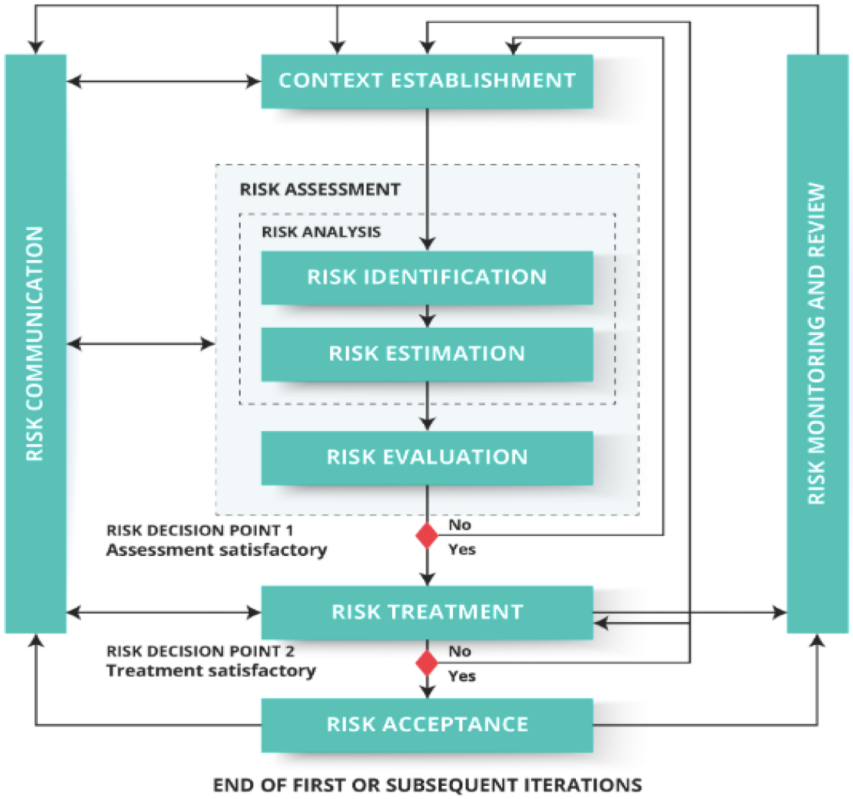
Authorize

Authorize system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and so on

ISO 27005 Overview

ISO 27005 Risk Management Workflow:-

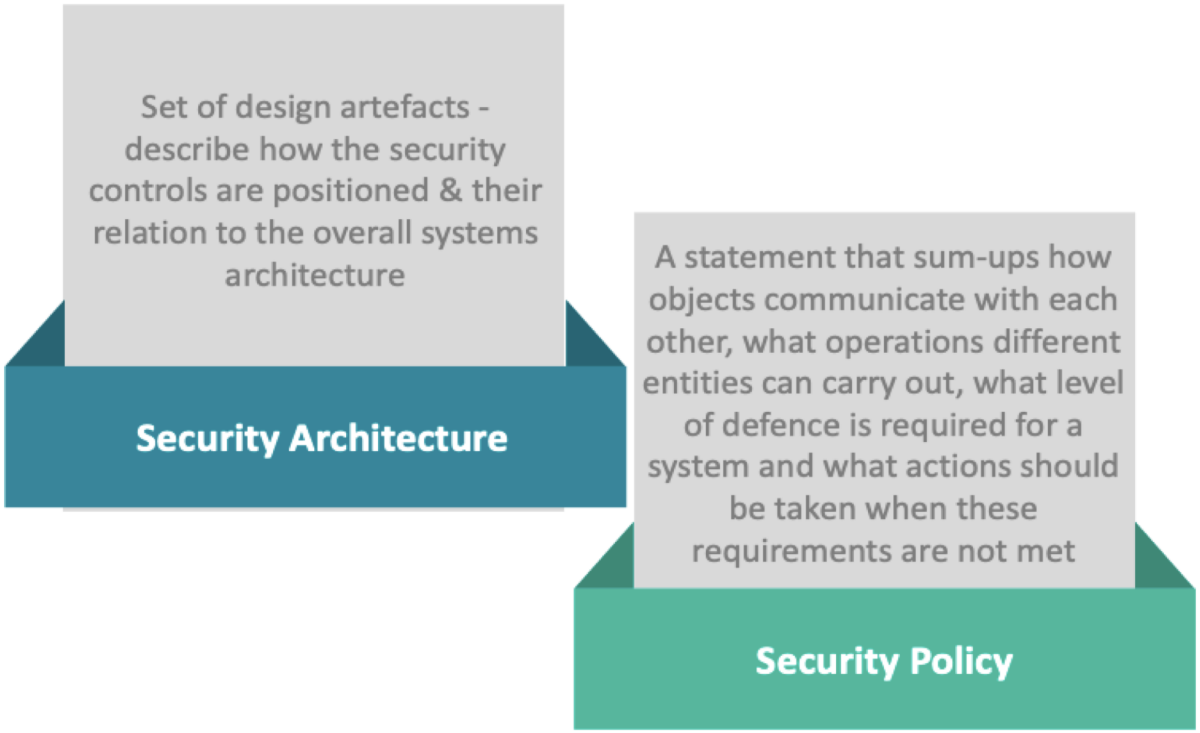
1. Design Controls based on risks clearly understood & measured given existing threats that could potentially exploit vulnerabilities to organizational assets
2. Systematic deployment of controls to reduce risks to an acceptable level of residual risk after approval by business leadership
3. Manage controls to maintain an acceptable level of mitigation
4. Provide ongoing analysis of controls to confirm continued effectiveness in light of changing operational conditions




That's all for Risk Management and its Framework. Now let us understand the Security Architecture

Security Architecture

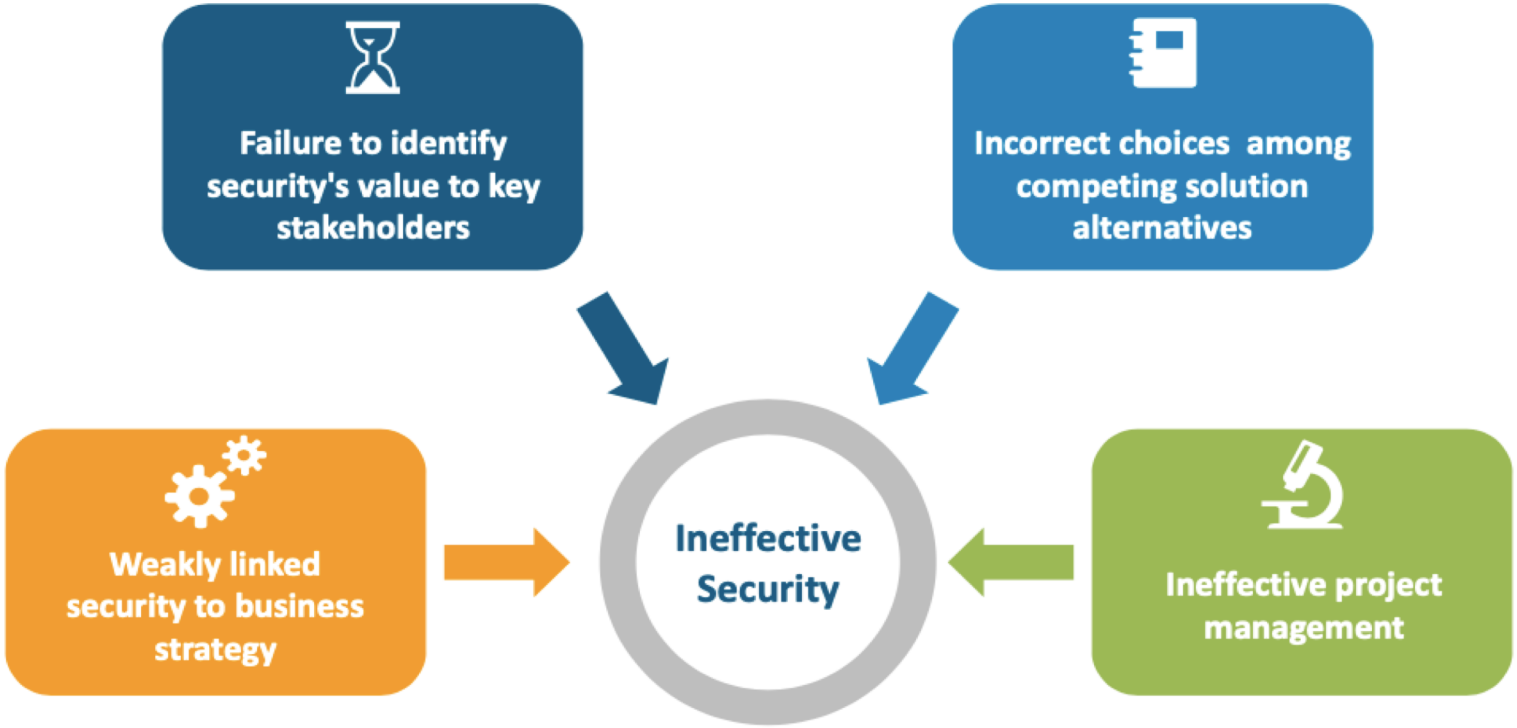
Top View For Security Architecture



Weak Information Security: Symptoms

- Incongruent security administration processes
- Redundant or intersecting security tools
- Difficulty getting funding and approval for security initiatives
- Audit findings and lengthy audit proceedings
- Tools not operational or not well accepted by users

What Is Weak Information Security ?



Enterprise Architecture

EA:

Enterprise Architecture (EA) is a process of translating business vision & strategy into an effective enterprise change by – creating, communicating & improving the key principles and models that describe the enterprise's future state and enable its evolution

EISA:

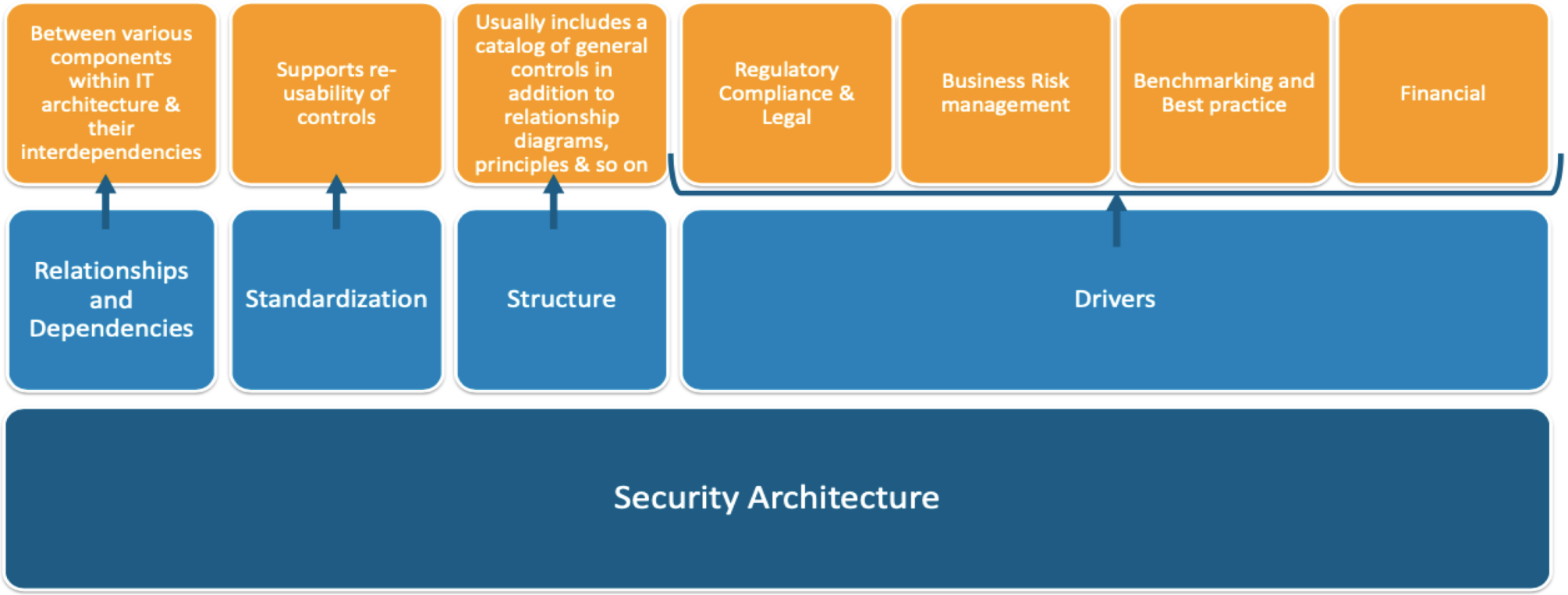
Enterprise Information Security Architecture (EISA) is the process that delivers planning, design and implementation documentation (artefacts) in support of the Information Security program

Security Architecture

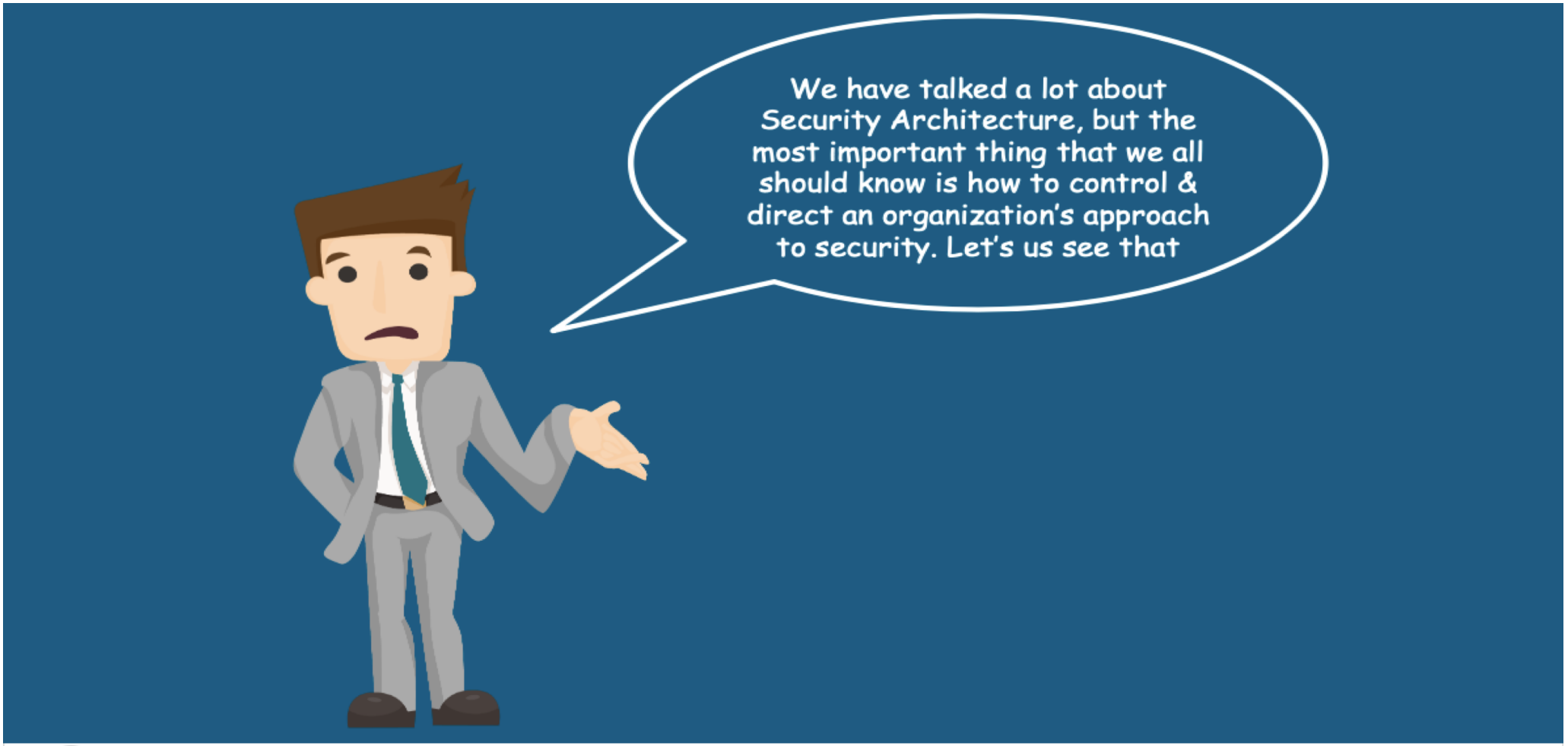
- Security Architecture is a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. It also specifies when and where to apply security controls. The design process is generally reproducible

- In Security Architecture, the design principles are reported clearly, and in-depth security control specifications are generally documented in independent documents. System architecture can be considered a design that includes a structure and addresses the connection between the components of that structure

Key Attributes Of Security Architecture



Key Phases In Security Architecture Process


We have talked a lot about Security Architecture, but the most important thing that we all should know is how to control & direct an organization's approach to security. Let's us see that

Security Governance

What Is Security Governance?

Security governance is the means by which you control & direct an organization's approach to security

Effective Security governance will successfully coordinate the security activities within an organization

It enables the flow of security information and decisions around your organization

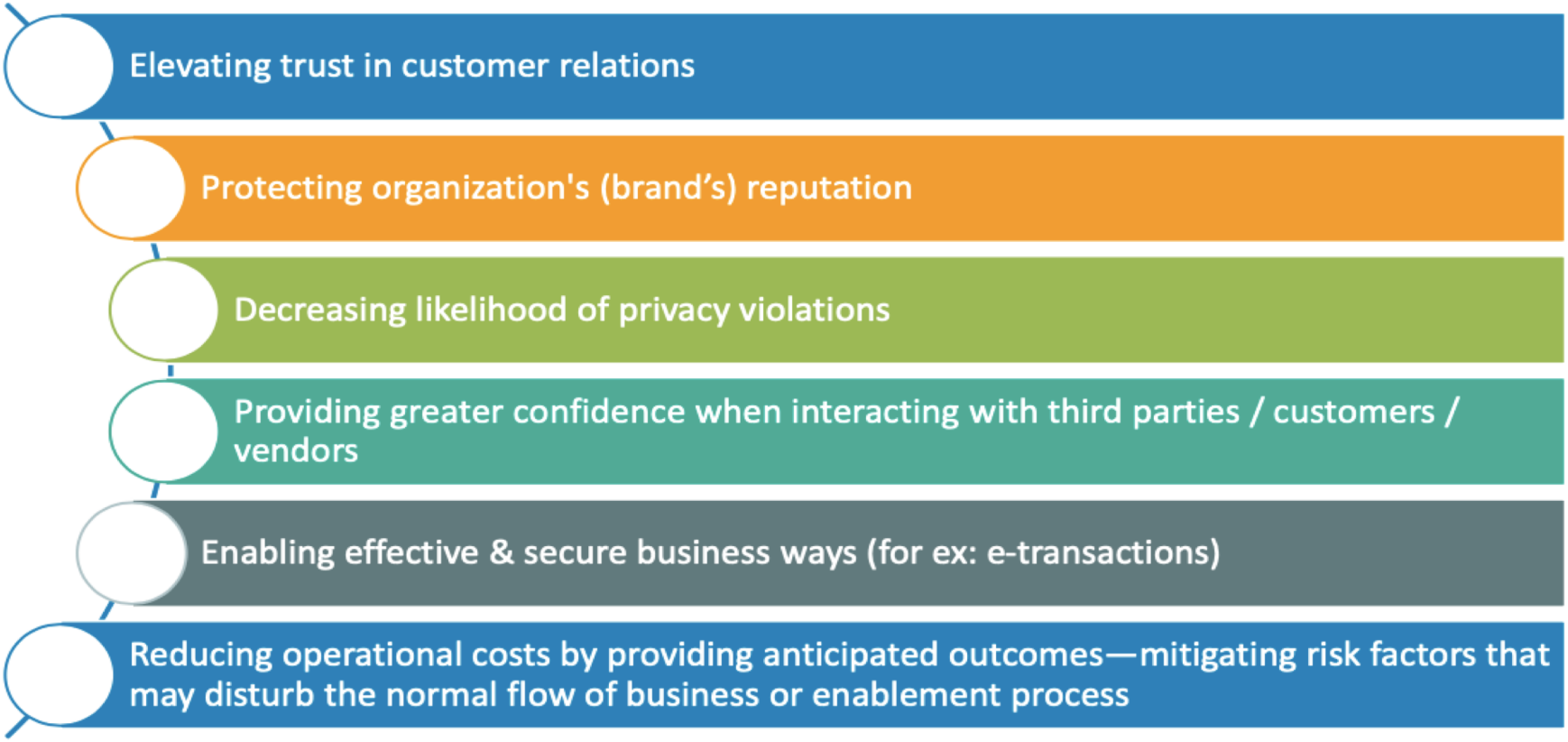
Security decision making can happen at all levels

An organization's senior leadership should use security governance to set out the kinds of security risks they are prepared for staff to take Vs. those they are not

Information Security Governance

- Information Security Governance is the responsibility of the board of directors and senior executives
- It must be an integral and transparent part of enterprise governance and be aligned with the IT governance framework

Benefits Of Information Security Governance



Security Auditing

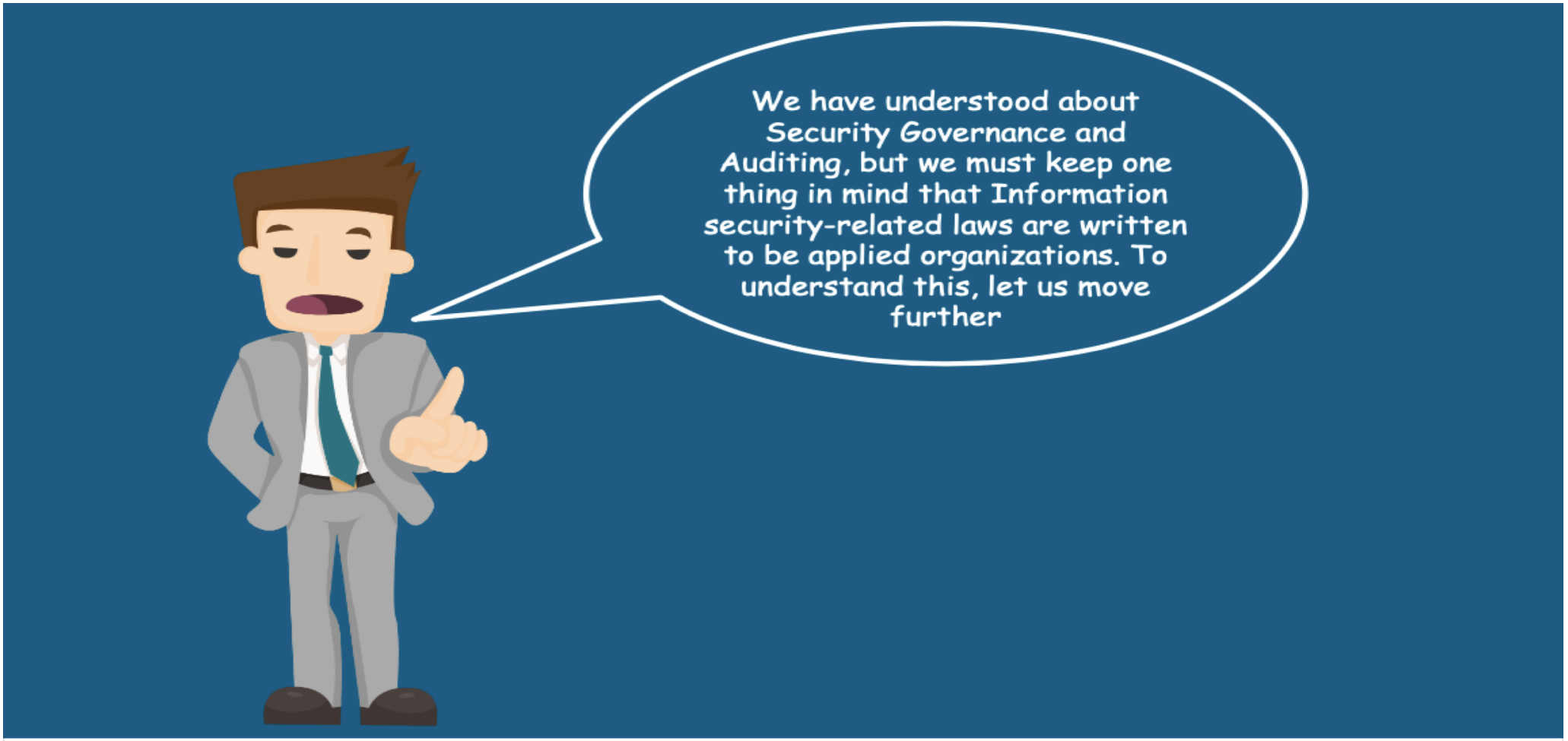
What Is Auditing?

An **audit** is a **systematic and independent inspection** of processes, books of accounts, statutory records, documents and vouchers of an organization to ascertain how far the financial statements as well as non-financial disclosures present a true and fair view of the concern with respect to declared references and regulations (as applicable)

Information Security Auditing

- An **Information Security Audit** is an audit on the standing of information security in an organization
- There are multiple types of audits, multiple objectives for different audits in the wide realm of an information security audit

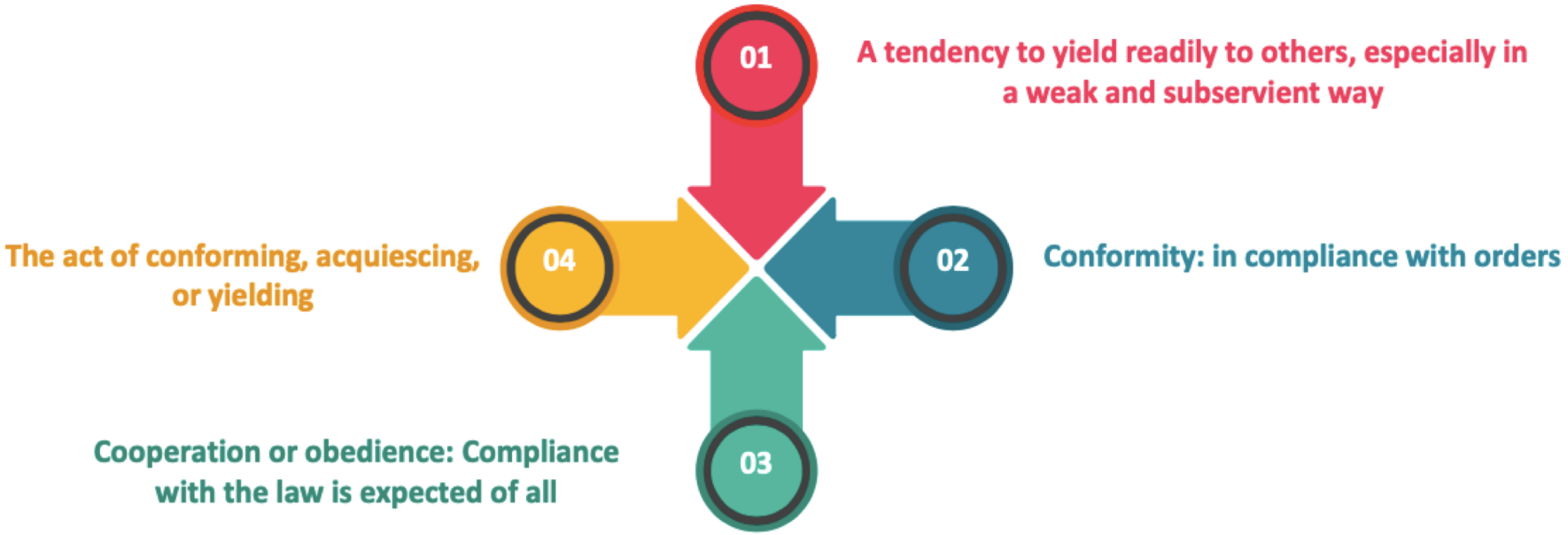
- Information security audits may cover :
  - Information assets
  - Physical security of data centers & data storing assets
  - Logical security of databases , classified data processing units/applications and so on
  - Control audits with reference to **regulations** such as GDPR, Data privacy laws and so on & **frameworks** such as ISO 27001, NIST and so on, depending on the type of business and its compliance drivers


We have understood about Security Governance and Auditing, but we must keep one thing in mind that Information security-related laws are written to be applied organizations. To understand this, let us move further

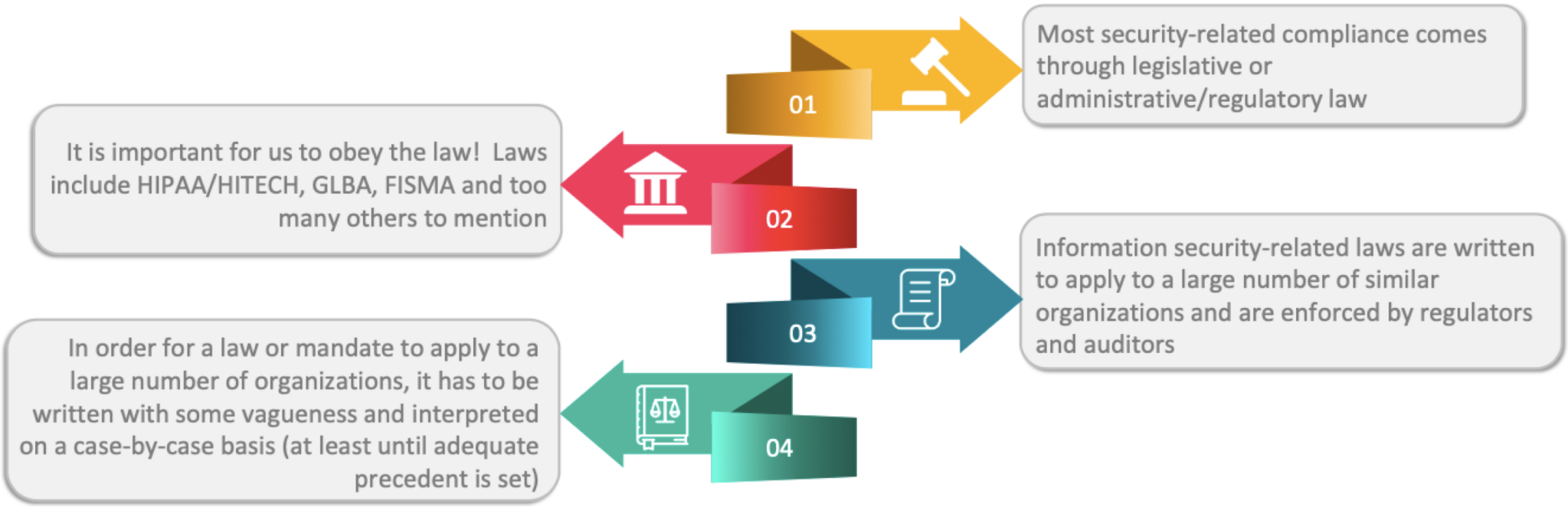
Compliance

What Do You Mean By Compliance?

"Compliance" definition by dictionary is as follows:-



Compliance: From A Security Standpoint



Need For Compliance

Most major organizations maintain compliance with at least one IT security regulation. Not only are many of these regulations mandatory, but they also greatly benefit them

Improve Security

IT security regulations improve corporate security measures by setting baseline requirements. This baseline keeps business data-security levels relatively consistent within respective industries

Increase Control

Improved security goes hand-in-hand with increased control. Prevent employee mistakes and insider theft with heightened credentialing systems while keeping an eye on outside threats

Minimize Losses

Improved security, in turn, prevents breaches, which are costly to businesses. Many companies end up losing millions in sales, repair costs and legal fees, all of which can be avoided with the right preventive measures

Maintain Trust

Customers trust businesses with their information. Honour that trust with improved security systems that keep their information safe

Common IT Security Compliance Regulations

GDPR

General Data Protection Regulation(GDPR) aims to protect citizens in the **European Union** (EU) from data breaches. GDPR applies to all companies processing personal data for people residing in the EU, even if that company is not physically located or based in the EU

HIPAA

Health Insurance Portability and Accountability Act is about healthcare & patients' data security. Any company that handle healthcare data, are required to comply with HIPAA regulations while handling data

SOX

Complying with the **Sarbanes-Oxley Act** involves maintaining financial records for seven years and it is required for U.S. company boards, management personnel and accounting firms. The point of the regulation was to prevent another incident like the Enron scandal, which hinged on fraudulent bookkeeping

FISMA

Federal Information Security Management Act of 2002 treats information security as a matter of national security for federal agencies. As part of the bill, all federal agencies are required to develop data protection methods

PCI-DSS

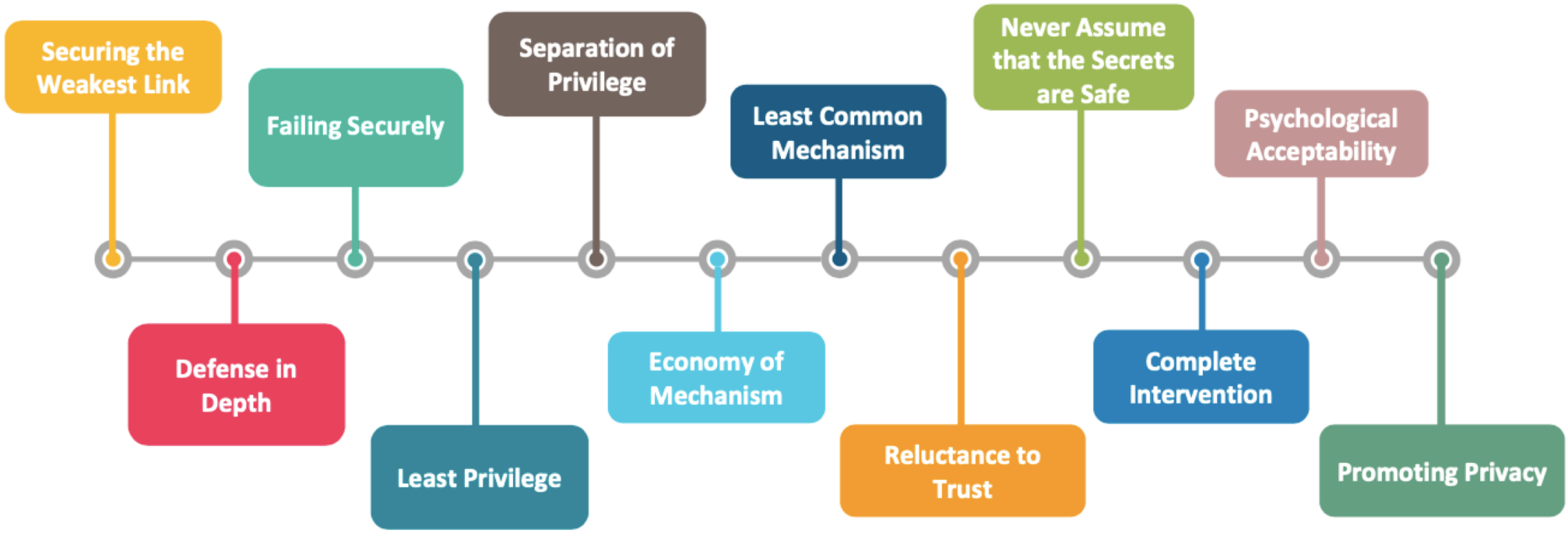
Payment Card Industry Data Security Standard is a set of regulations meant to help reduce fraud, primarily through protecting customer credit card information. PCI-DSS security and compliance is required for all companies handling credit card information

GPG13

Good Practice Guide 13 is a U.K. general data protection regulation for business processes. This system is implemented by many organizations, but is compulsory for those managing high-impact data

Basic Concepts Of Secure System Design

Secure Design Principles



FTVETI

ICT @ FTVETI

Security – Design Techniques

Threat Modeling

It is a structured approach for analysing the security of an application. It helps to identify, quantify, & address the security risks associated with an application

Risk Assessment

It is a discipline of methodically finding hazards, evaluating their impact and choosing treatment options

Evaluation Criteria

A benchmark against which accomplishment, conformance, performance, & suitability of an individual, alternative, activity, product, plan, as well as of risk-reward ratio is measured

Secure Coding

It is the practice of developing computer software in a way that guards against the accidental introduction of security vulnerabilities

Vulnerability Assessment

A vulnerability assessment is the testing process used to identify & assign severity levels, to as many security defects as possible in a given timeframe

Formal Methods

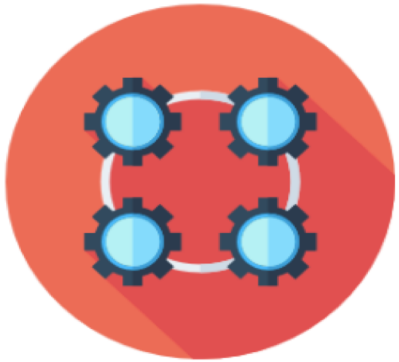
It enables modelling, verifying, & synthesizing computer systems. Logical or mathematical descriptions of entities enable drawing reliable conclusions about their behaviour

Cryptographic Techniques

It includes encryption, decryption and cryptographic hashing

Security Patterns

- A **Security Pattern** condenses security knowledge in the form of pre-worked solutions to recurring security problems, presenting issues and trade-offs in the usage of the pattern
- There are two types of security patterns :



Procedural Patterns

Structural Patterns

Examples Of Procedural Security Patterns

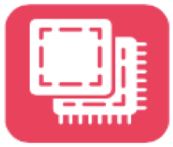
Building the Server from the Ground Up

Enrolment by Validating Out of Band

Logging for Audit

Choosing the right alternative

Enrolment using Third-Party Validation



Patching Pro-actively

Documenting Security Goals

Enrolment with a Pre-existing Shared Secret

Red Teaming the Design

Documenting Server Configuration

Enrollment without Validation

Sharing Responsibility for Security

Examples Of Structural Security Patterns


Account Lockout


Network Address Blacklist


Password Transmission


Manage Authenticated Session


Client Data Storage


Secure Assertion


Client Input Filters


Partitioned Application


Server Sandboxing


Encrypted Storage

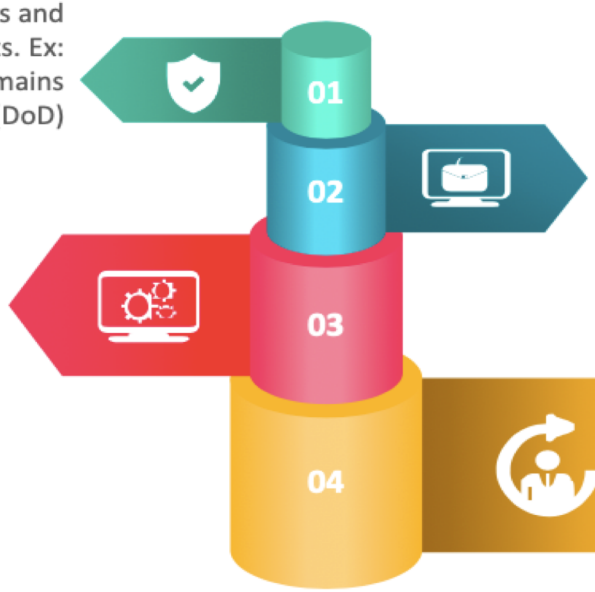

Password Authentication


Trusted Proxy & Transaction validation

Security Domains

Security Domain

Security domain is the list of objects, a subject is allowed to access. Domains are groups of subjects and objects with similar security requirements. Ex: Confidential, Secret, Top Secret are 3 security domains used by the U.S. **Department of Defence** (DoD)



OS Kernel

Kernel is a computer program that is the core of a computer's operating system, with complete control over everything in the system. With respect to computing, two frequently observed security domains are **User mode** and **Kernel mode**

Kernel Mode

Kernel mode (supervisor mode) is where the kernel lives, allowing low-level access to memory, CPU, disk and so on. It is the most trusted and powerful part of the system

User Mode

User accounts & their processes live into User Mode. The two domains are separated: an error or security lapse in user mode should not affect the kernel


One important topic that we need to cover is "Ring Model". Let's understand what a ring model is

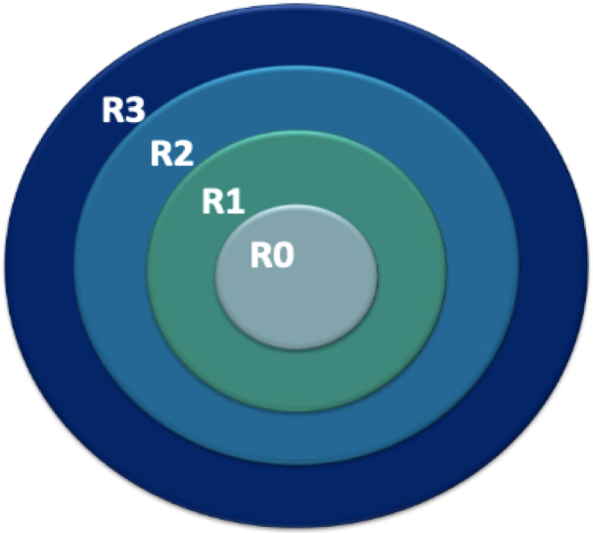
Abstraction | Ring Model

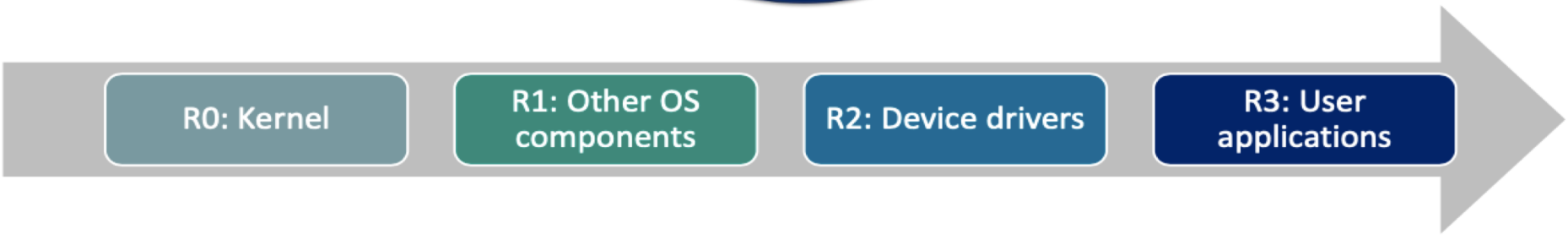
The **Ring Model** is a form of CPU hardware layering that splits and defends domains (Kernel mode and User mode) from each other

Many CPUs, such as the Intel X86 family, have four rings, ranging from ring 0 (Kernel) to ring 3 (user)

The deepest ring is the most trusted, and each successive outer ring is less trusted

Ring Model View





Quizzes

Quiz #1

- An organization found that one of it's customer is facing a problem with the application. The Application built on standard technology stack got breached and the customer's password data was leaked & published to the dark web! What was not most probably not timely worked on, by the organization's IT team?
  a. Threat Analysis
  b. Vulnerability management
  c. Risk Analysis
  d. Compliance Audit

Answer #1

- An organization found that one of it's customer is facing a problem with the application. The Application built on standard technology stack got breached and the customer's password data was leaked & published to the dark web! What was not most probably not timely worked on, by the organization's IT team?
  a. Threat Analysis
  b. Vulnerability management
  c. Risk Analysis
  d. Compliance Audit

Answer b:
Explanation: Vulnerability management keeps a track of timely identification & mitigation of vulnerabilities in a given system. Either patching or virtual patching for the open vulnerabilities ensure they not getting exploited

Quiz #2

- A hacker while trying to manually brute force (use some commonly known passwords) to gain unauthorized root access to a public desktop, keeps getting a warning message. It does not however, technically stop the attacker from continuing brute forcing attempts. What kind of control is depicted by the warning message?
  a. Preventive control
  b. Detective control
  c. Corrective control
  d. Deterrent control

Answer #2

- A hacker while trying to manually brute force (use some commonly known passwords) to gain unauthorized root access to a public desktop, keeps getting a warning message. It does not however, technically stop the attacker from continuing brute forcing attempts. What kind of control is depicted by the warning message?
  a. Preventive control
  b. Detective control
  c. Corrective control
  d. Deterrent control

Answer d:
Explanation: A deterrent control aims to deter (discourage) an attacker or a malicious individual to perform the malicious activity. However, it is not a technical control to detect or correct the damage

Quiz #3

- A classic pointer to a weak Information Security program in an organization is:
  a. Procedures are not compliant
  b. Information Security Governance is either not implemented well or not effective
  c. Internal audit is not performing well
  d. Lack of Cyber Security insurance

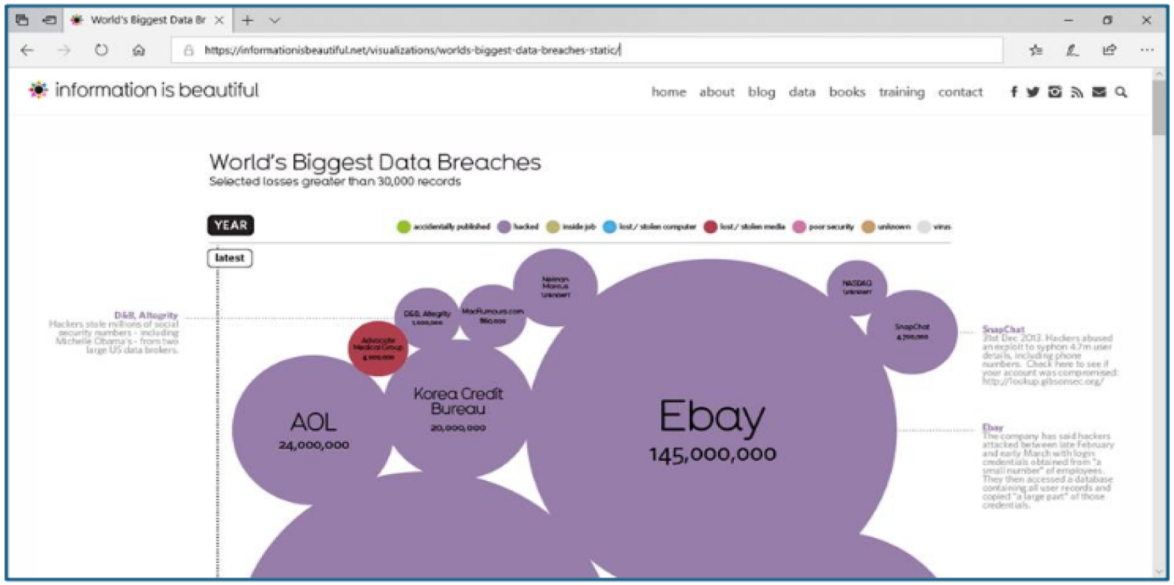
Answer #3

- A classic pointer to a weak Information Security program in an organization is:
  a. Procedures are not compliant
  b. Information Security Governance is either not implemented well or not effective
  c. Internal audit is not performing well
  d. Lack of Cyber Security insurance

Answer b:
Explanation: Info Sec governance is the responsibility of the top management & board. The effectiveness of Info Sec Governance activity is the key element that reflects the security posture of an organization. Without efficient, effective & appropriate information security governance - the overall information security program remains half hearted and thus does not work well

Demo 1: Data Breaches

- Study the world's biggest data breaches in various industry sectors
- Filter the data based on methods of leak and number of records stolen
- Use the link: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-static/

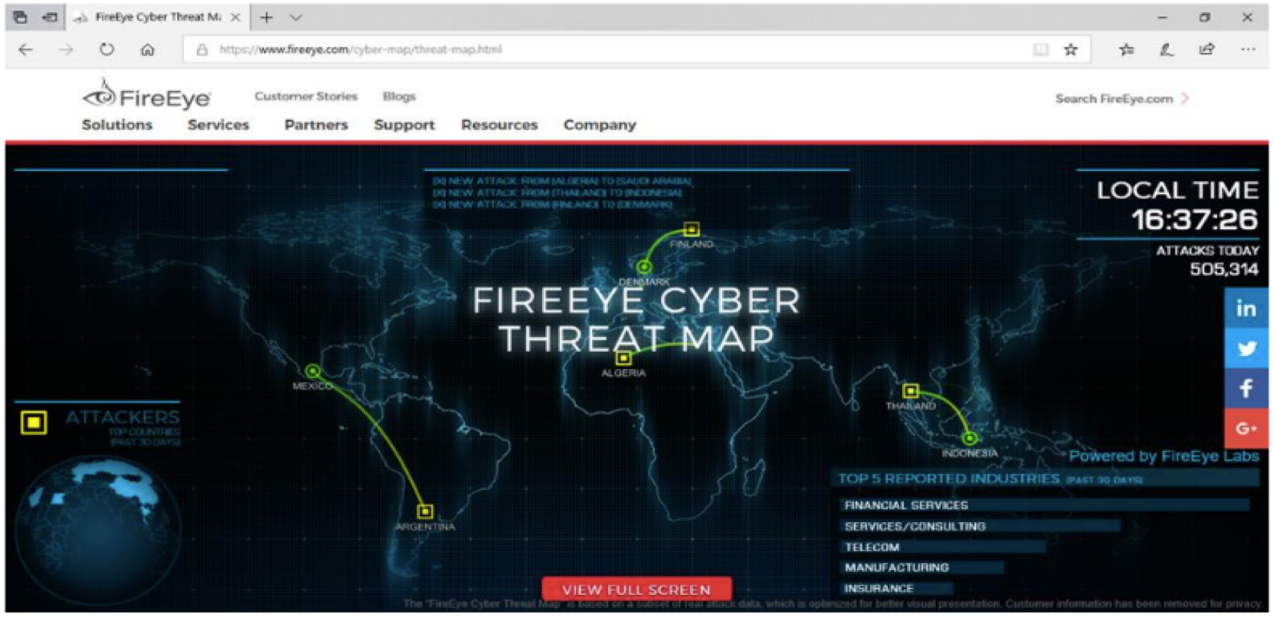


FTVETI

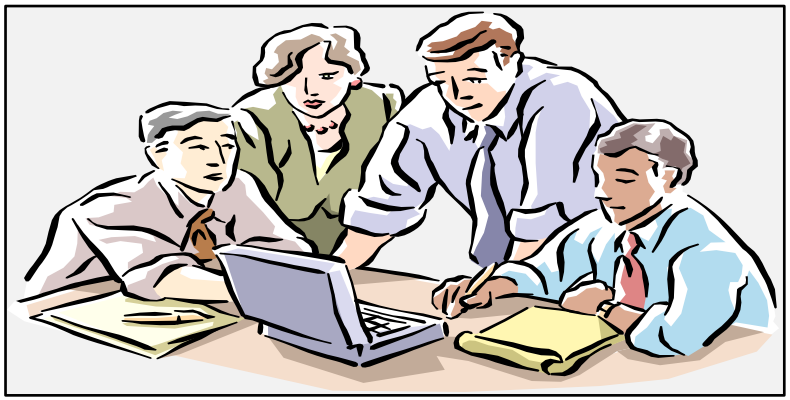
ICT @ FTVETI

Demo 2: Internet Threat Scenario

- Monitor the global cyber threat scenario including hacking, bots, and malware attacks using live threat maps
- Identify hacking attempts or cyber-attacks from different parts of the world as they happen in real time
- Use the link: https://www.fireeye.com/cyber-map/threat-map.html



QUESTIONS PLEASE ☺



FTVETI