Introduction to Cybersecurity

Incident Management

Learning Objectives

By the end of this lesson, you will be able to:

- Develop an incident management and response system
- Explain the process of digital forensics
- Describe business continuity and disaster recovery

Developing an Incident Management and Response System

Incident

It is an adverse event that can cause damage to an organization’s assets, reputation, or personnel.

Incident Management

The process of developing and maintaining the capability to manage incidents within an organization.

Incident Response

It is the capability to effectively prepare for and respond to unanticipated events to control and limit damage and maintain or restore normal operation.

Incident vs Incident Response

Incident

Unplanned interruption to an IT service

Incident Management

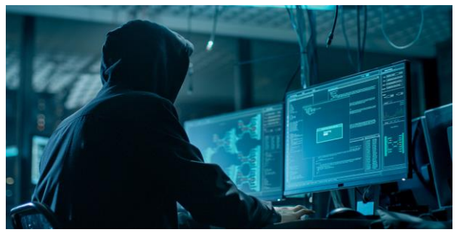
This process ensures that:

- Normal service operation is restored
- Business impact is minimized

Incident Response Plan

It is a set of instructions to help IT staff detect, respond to, and recover from network security incidents.

These types of plans address issues like:



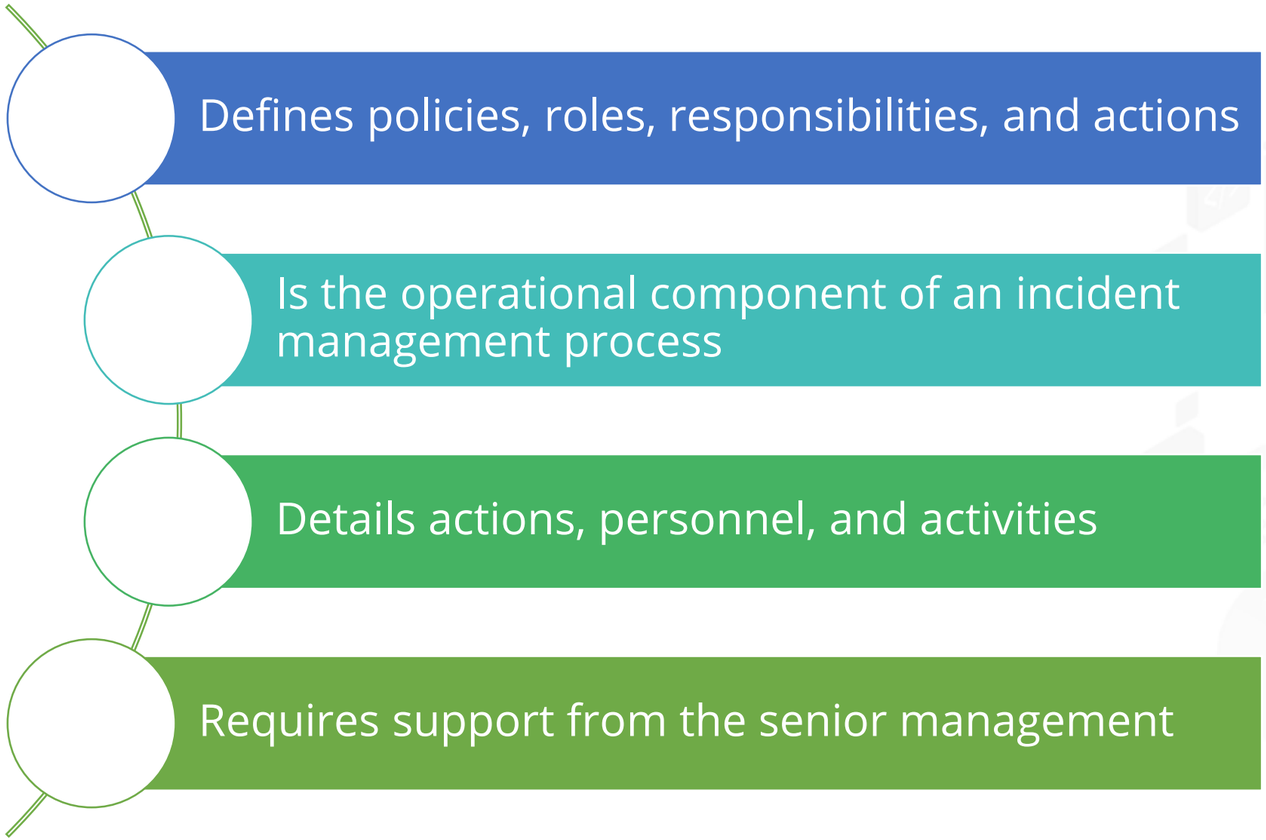
Cybersecurity

Data Loss

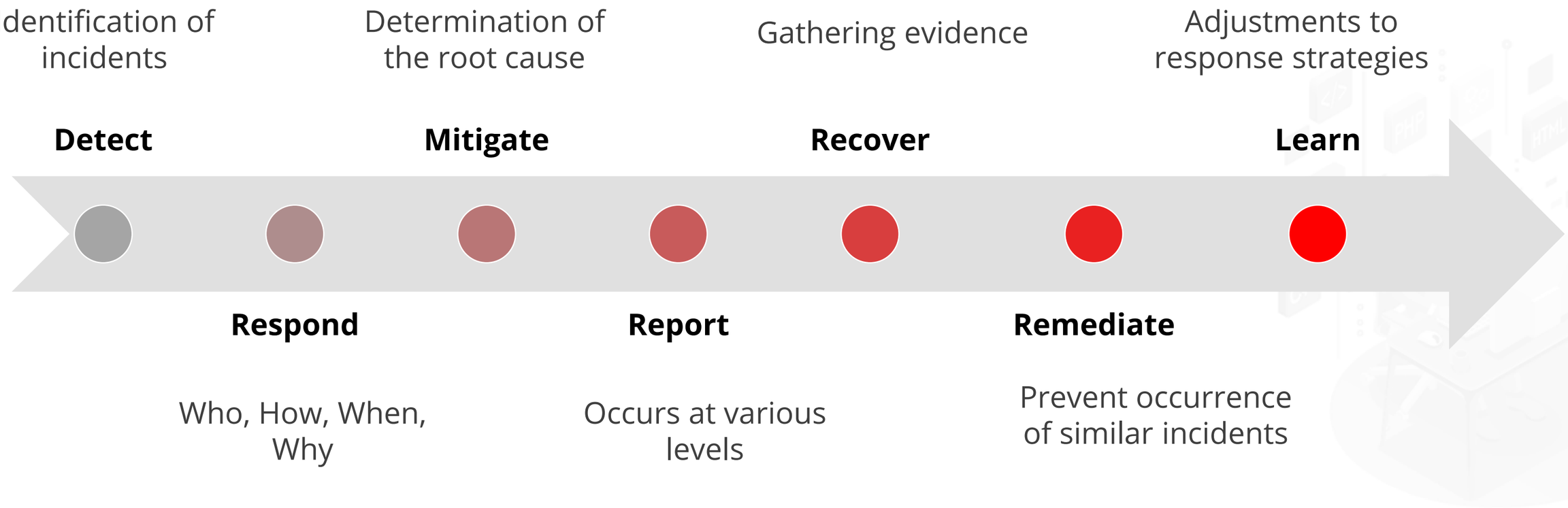
Service Outage

Incident Response Plan

Incident Response Plan



Incident Management Stages



Incident Response Metrics

Number of incidents

Dwell time

Time to contain the incidents

Time to resolve the incidents

Number of people affected

Total cost required to resolve the incident

Not meeting SLAs

Incident Management Team (IMT)

Team training prepares a group of individuals to function together as an Incident Management Team or IMT.

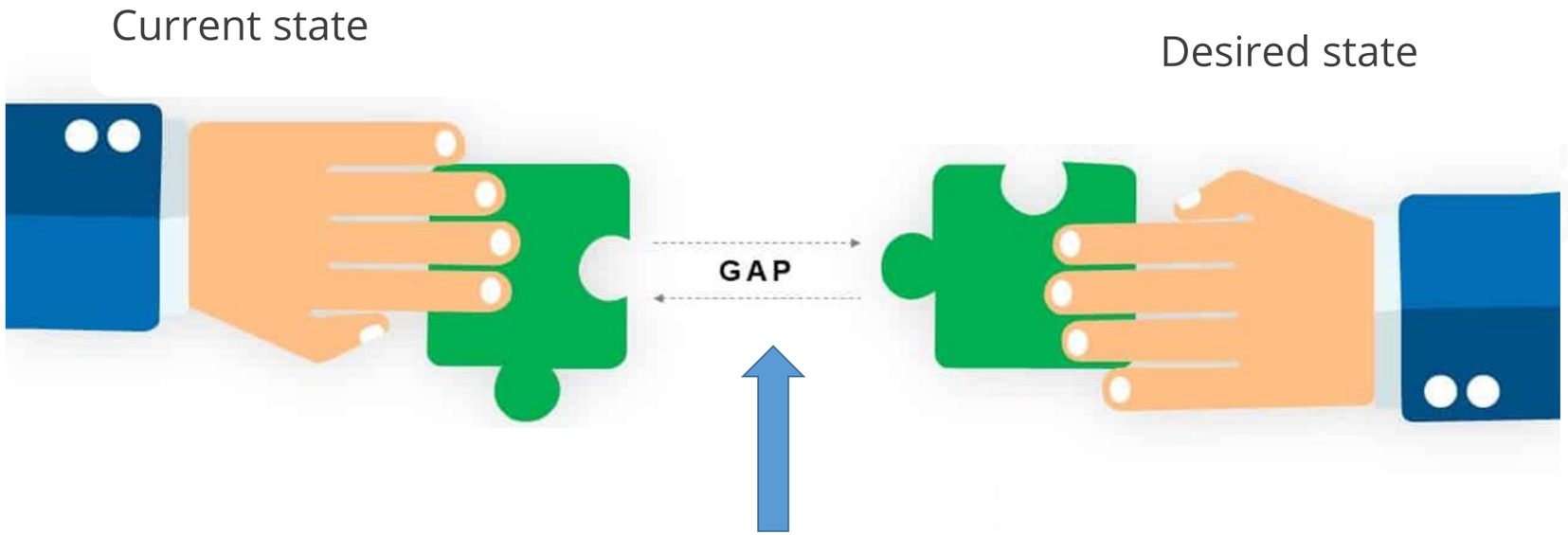
Incident Management Team

Incident Management Team (IMT)

Training programs for the IMT

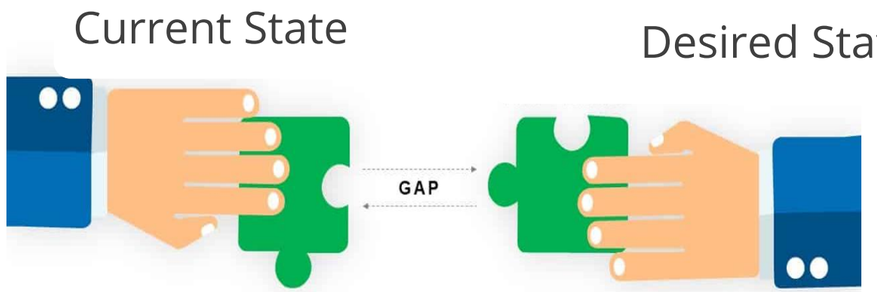
Gap Analysis

Assesses the differences in performance between a business information system and software applications



Gap analysis provides information on the actions required.

Gap Analysis



Compare the two levels to identify:

Processes that needs to be improved

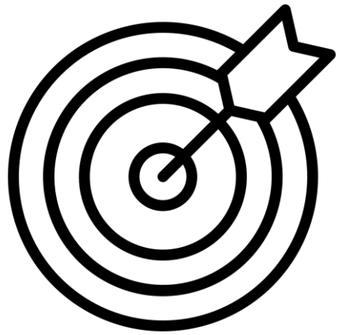
Resources needed to achieve the objectives

Digital Forensics

Digital Forensics

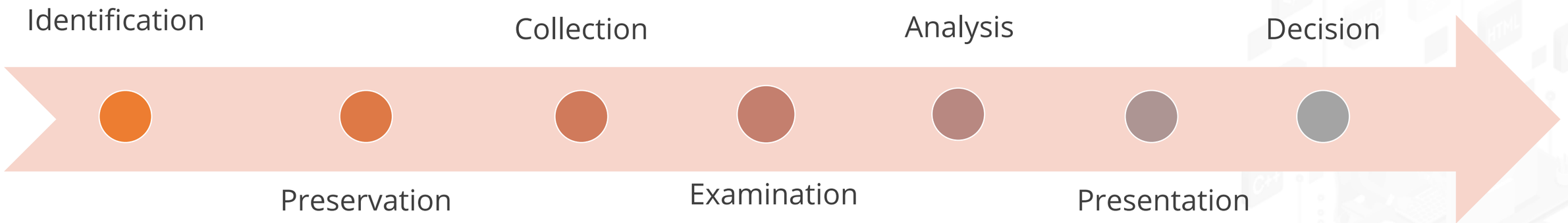
Digital forensics is the process of revealing and interpreting electronic data, which recovers and investigates the information found in digital devices.

Goal of Digital Forensics



Examine digital media to identify, analyze, preserve, recover, and present facts and opinions about digital information.

Forensics Investigation Process



Goal: Preserve any evidence in its most original form while performing a structured investigation.

Forensic Process Best Practices

Ask investigator to work only on the secondary image

Store the primary image in a library

Timestamp evidence to show when it was collected

Capture deleted files, slack spaces, and unallocated clusters through original image

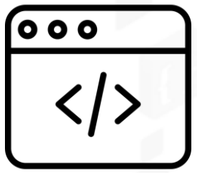
Ensure the destination is sanitized before collecting the images

Forensics Investigative Assessment Types

- Network analysis
- Media analysis
- Software analysis
- Hardware/Embedded device review

Traffic analysis

Log analysis



Path tracing

Forensics Investigative Assessment Types

- Network analysis
- Media analysis
- Software analysis
- Hardware/Embedded device review

Disk imaging

Timeline analysis

Registry analysis

Volume shadow analysis

Forensics Investigative Assessment Types

- Network analysis
- Media analysis
- Software analysis
- Hardware/Embedded device review

Reverse engineering

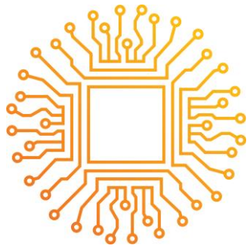
Malicious code review

Exploit review

Forensics Investigative Assessment Types

- Network analysis
- Media analysis
- Software analysis
- Hardware/Embedded device review

Dedicated appliance attack points



Firmware

Dedicated memory inspections

Digital Evidence

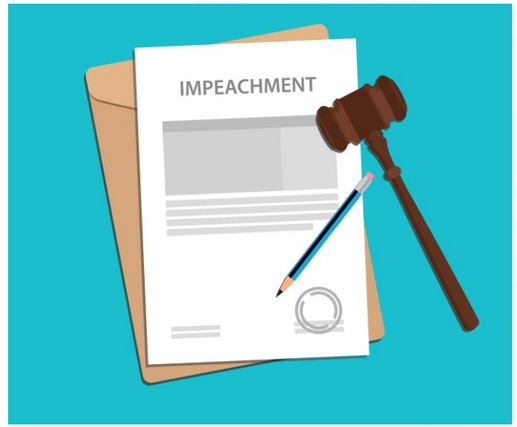
It is defined as information and data value to an investigation that is stored, received, or transmitted by an electronic device.

Digital Evidence

Stored and transmitted in a binary form

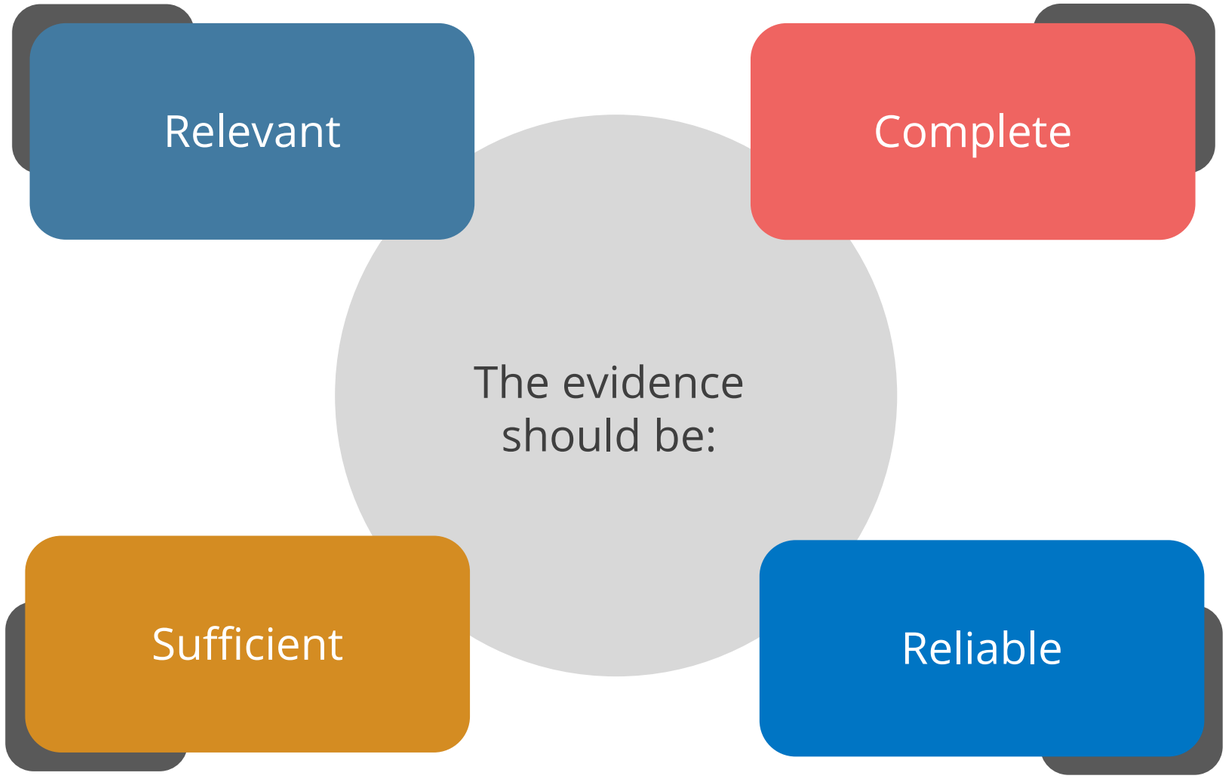
Is associated with electronic crime

Commonly found in digital devices



Used to prosecute crimes

Digital Evidence: Admissible in Court

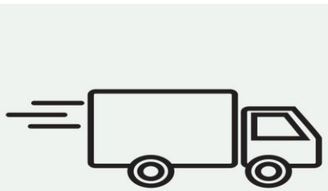


Evidence Life Cycle

Collection and identification

Presentation in court

Storage, preservation, and transportation



Return of evidence to owner

Chain of Custody

It is a chronological documentation developed from the information gathered at the crime scene.

Chain of Custody

It is a history that shows how the evidence was collected, analyzed, transported, and preserved

It should follow the evidence through its entire life cycle

The copies created should be independently verified and tamperproof

The evidence must be labeled with information of who secured and validated it

Business Continuity and Disaster Recovery (BCDR)

Business Continuity Planning and Disaster Recovery

Business continuity planning

Is having a plan to deal with major disruptions

≠

Disaster recovery

Is an organization’s ability to recover from a disaster

Seven Phases of a Business Continuity Plan

The seven phases of business of a business continuity plan is a complex arrangement of critical processes that allows continuation of business activities after an emergency.

7

Phases

Seven Phases of a Business Continuity Plan

Business Impact Analysis

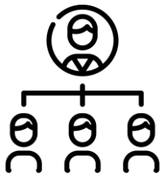
It is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations.

Disaster Recovery Sites

Acceptable risk

Key business processes

Risk tolerance



Structure and culture

Business impact analysis

Critical IT and physical resources

Disaster Recovery Sites

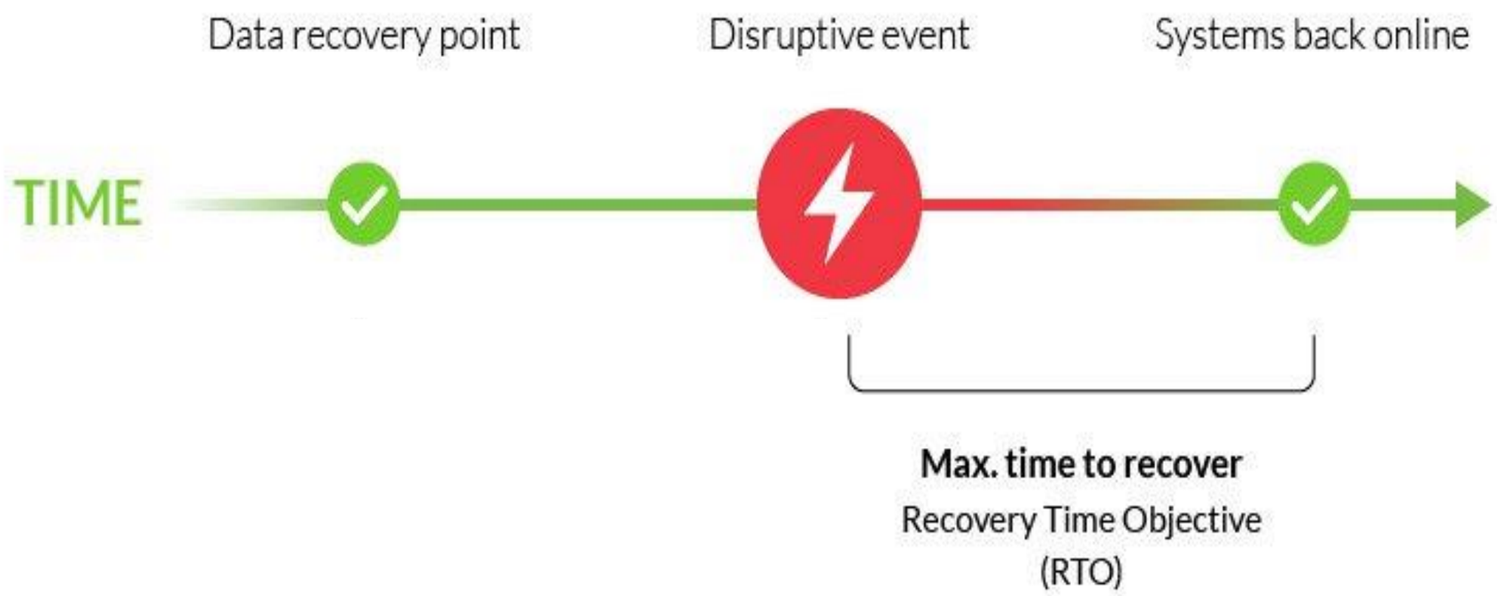
It is a facility that an organization uses to recover and restore its technology infrastructure and operations.

Recovery Point Objective (RPO)

Recovery Time Objective (RTO)

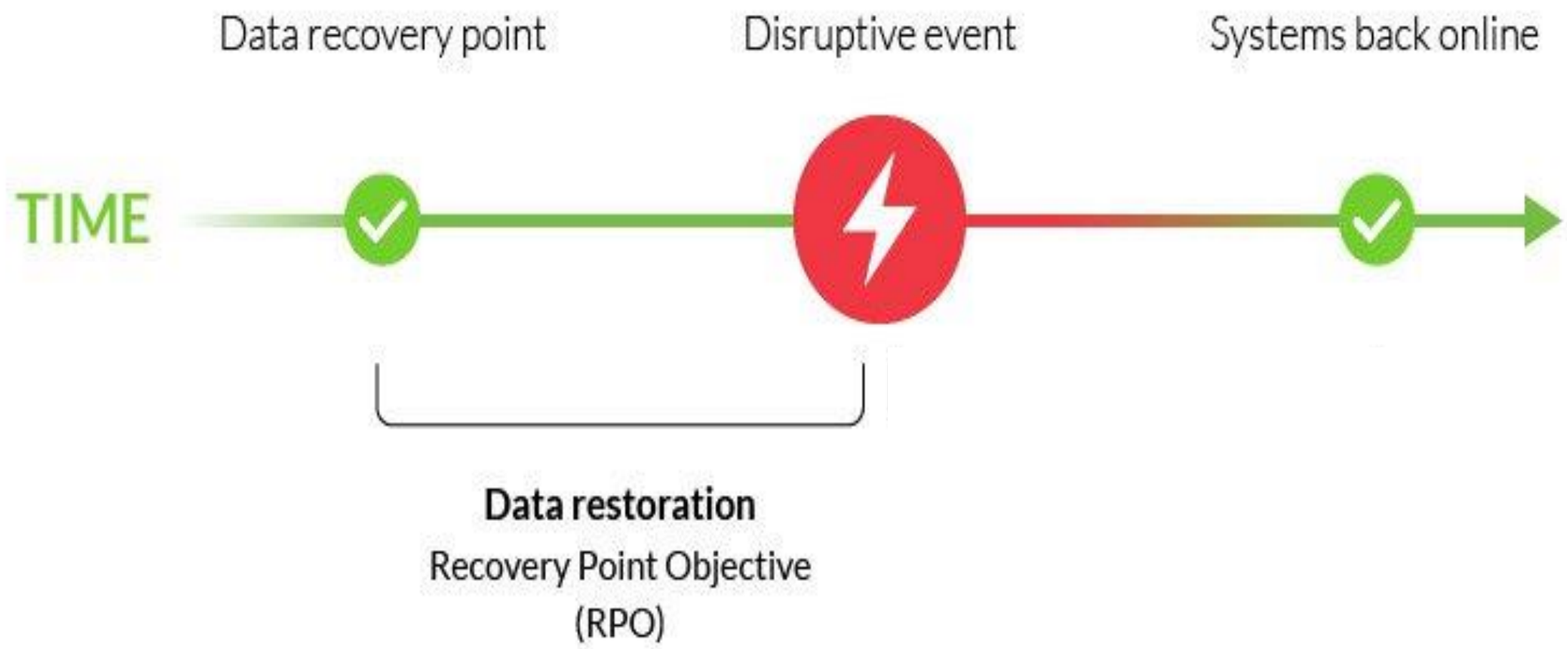
Recovery Time Objective

It is the maximum desired length of time allowed between an unexpected failure and the resumption of normal operations.



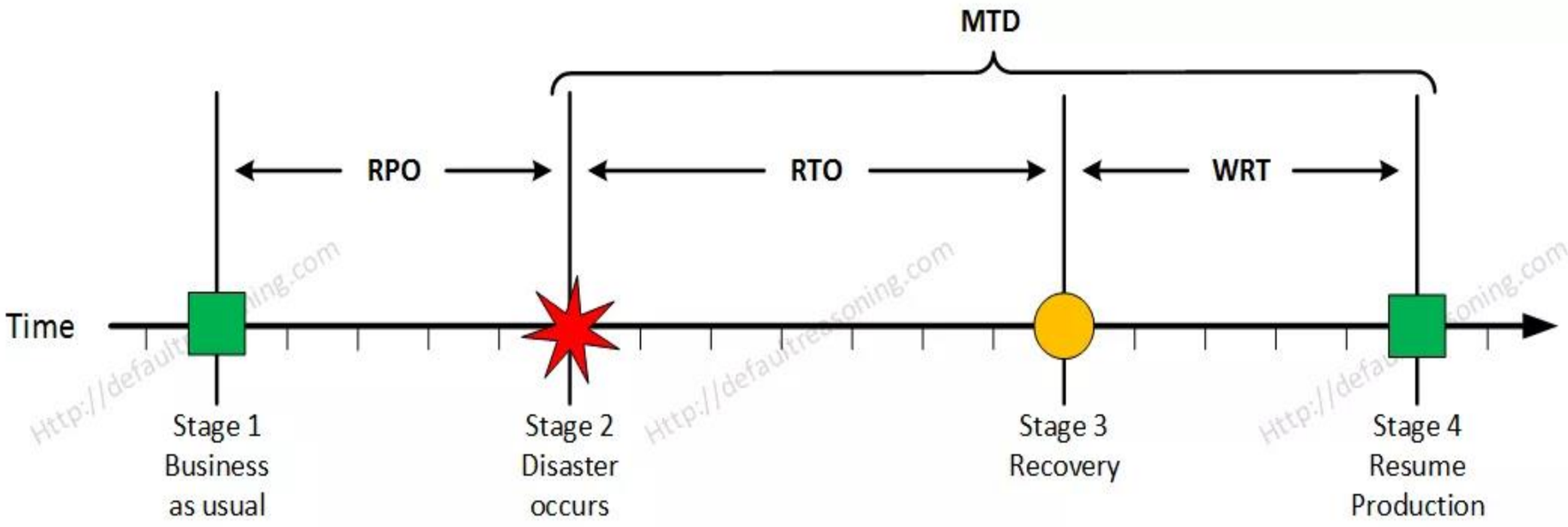
Recovery Point Objective

It is the maximum data loss from the onset of a disaster.



Maximum Tolerable Downtime

This is when the process is unavailable and creates irreversible consequences.



Types of Disaster Recovery Sites

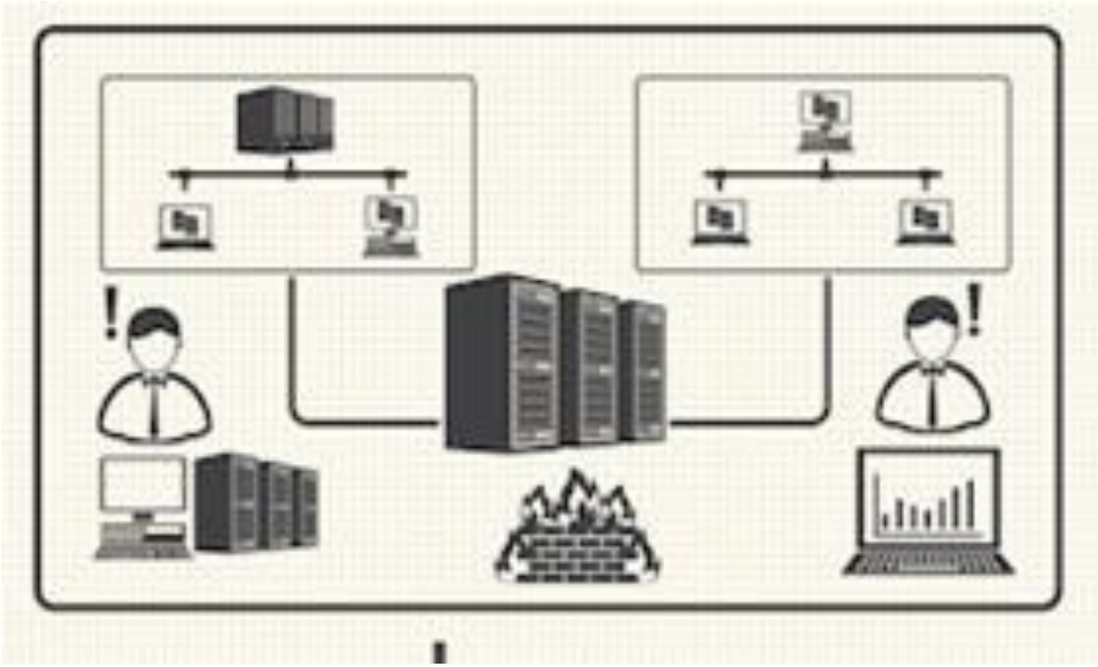
Cold site

Warm site

Hot site

Disaster Recovery Testing

It examines each step in the Disaster Recovery Plan.



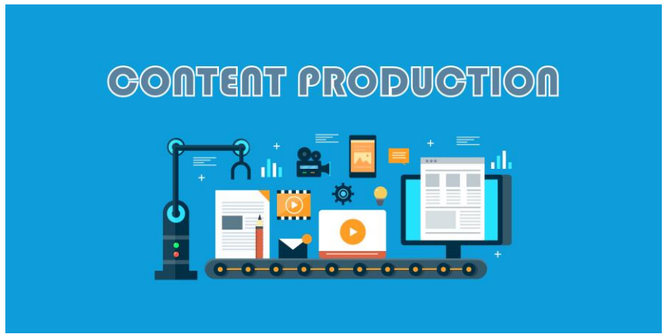
Types of Disaster Recovery Testing

Document review

Walk-through test

Simulation test

Parallel test

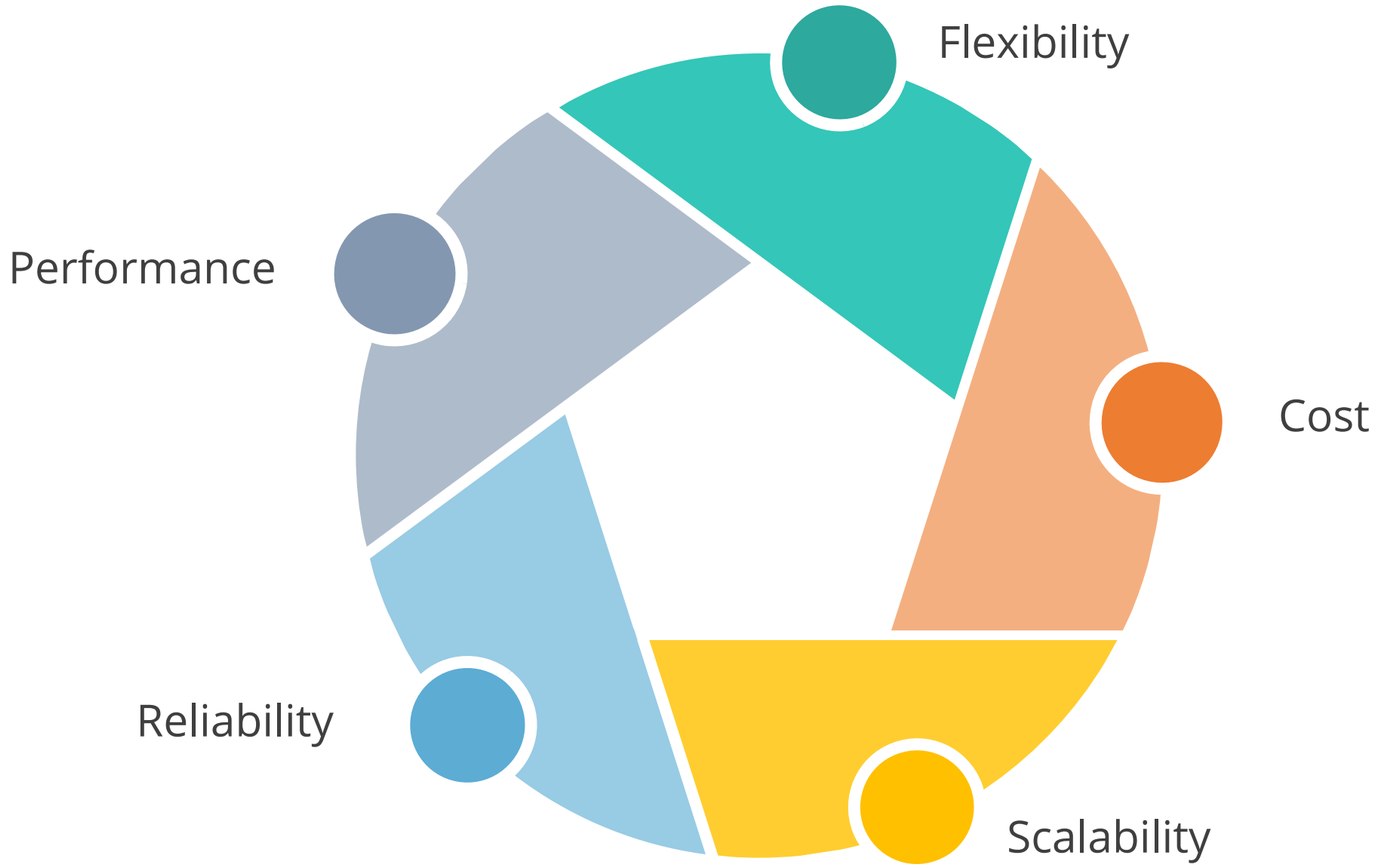


Cutover test

Cloud, Virtualization, BYOD, and IOT Security

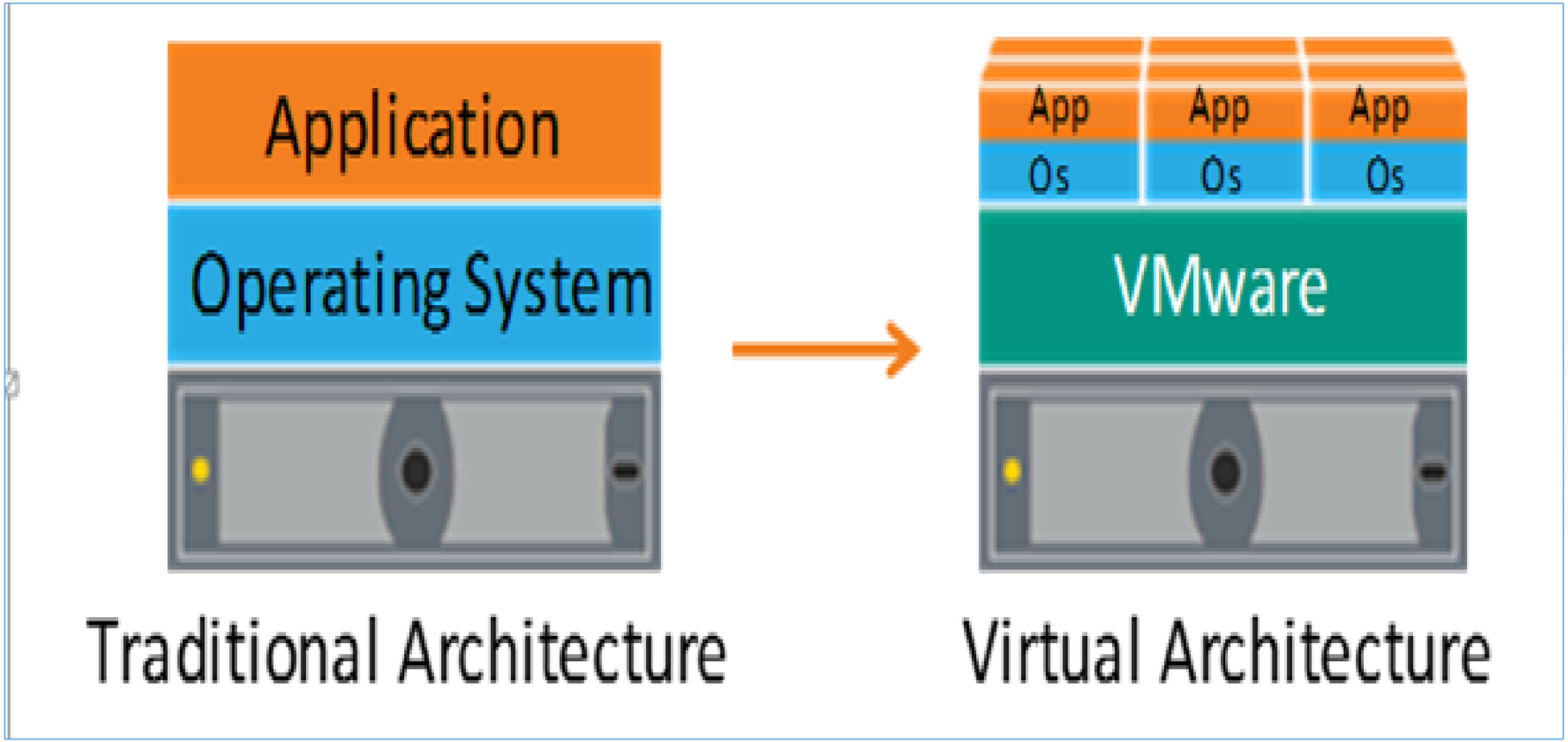
Virtualization

It is a technology that enables multiple operating systems to run side-by-side on same processing hardware.



Virtualization

It adds a software layer between an operating system and underlying computer hardware.



Virtualization

Pros

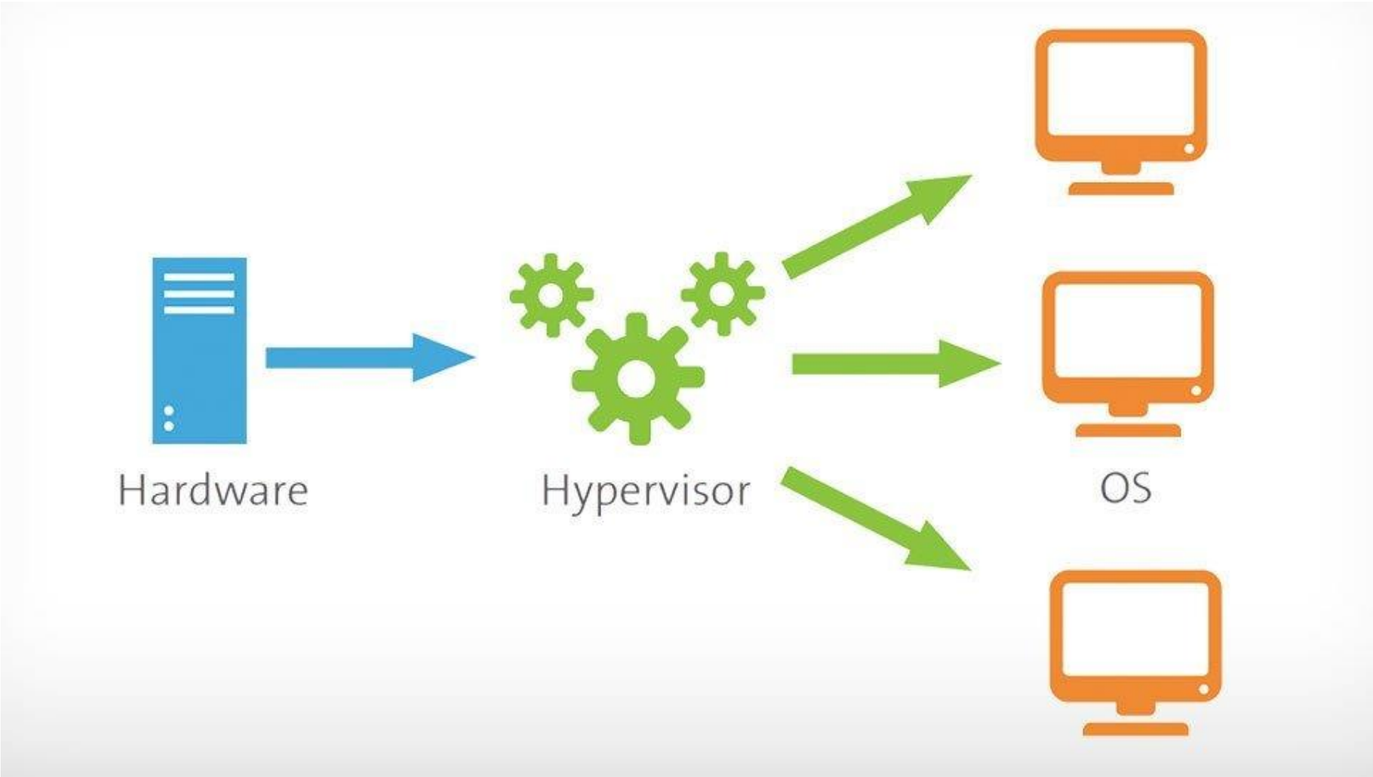
- Efficient
- Higher availability and lower cost

Cons

- Single point of failure
- Weaker in security and privacy

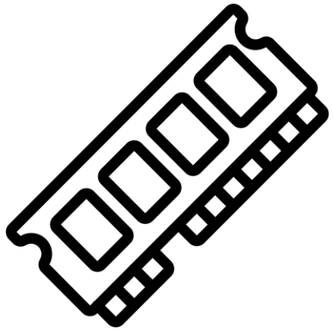
Hypervisor

It is a process that separates computer operating systems and applications from the physical hardware.



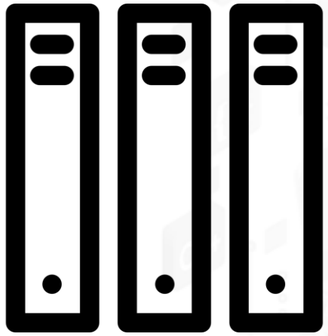
Hypervisor

It uses host machines to help maximize the effective use of computing resources.



Memory

Network bandwidth



CPU cycles

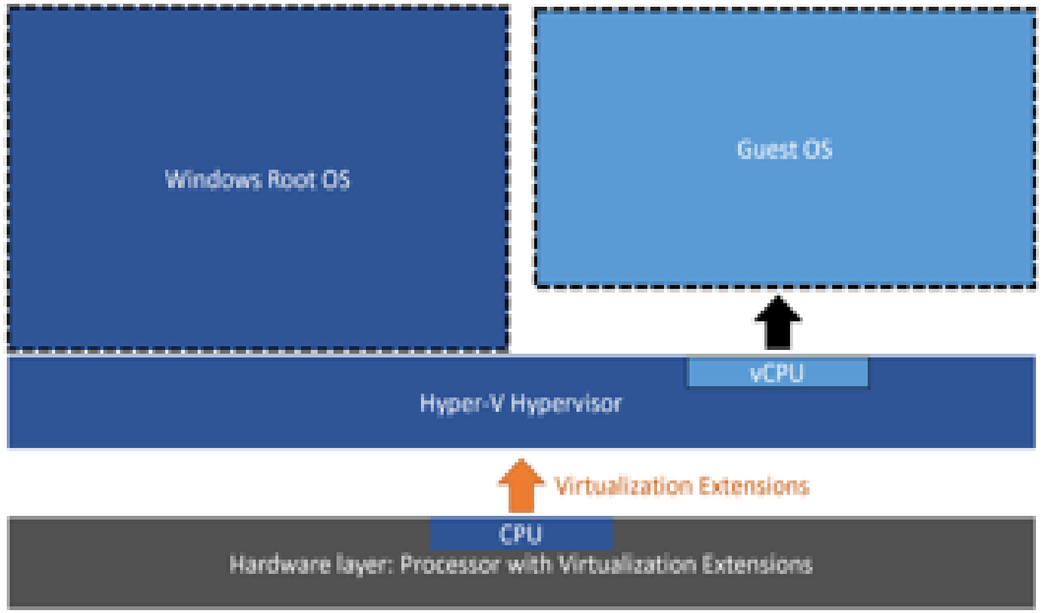
Hypervisor

Host-based virtual machine

It is an instance of a desktop operating system that runs on a centralized server.

Guest virtual machine

It refers to a virtual machine that is installed, executed, and hosted on the local physical machine.



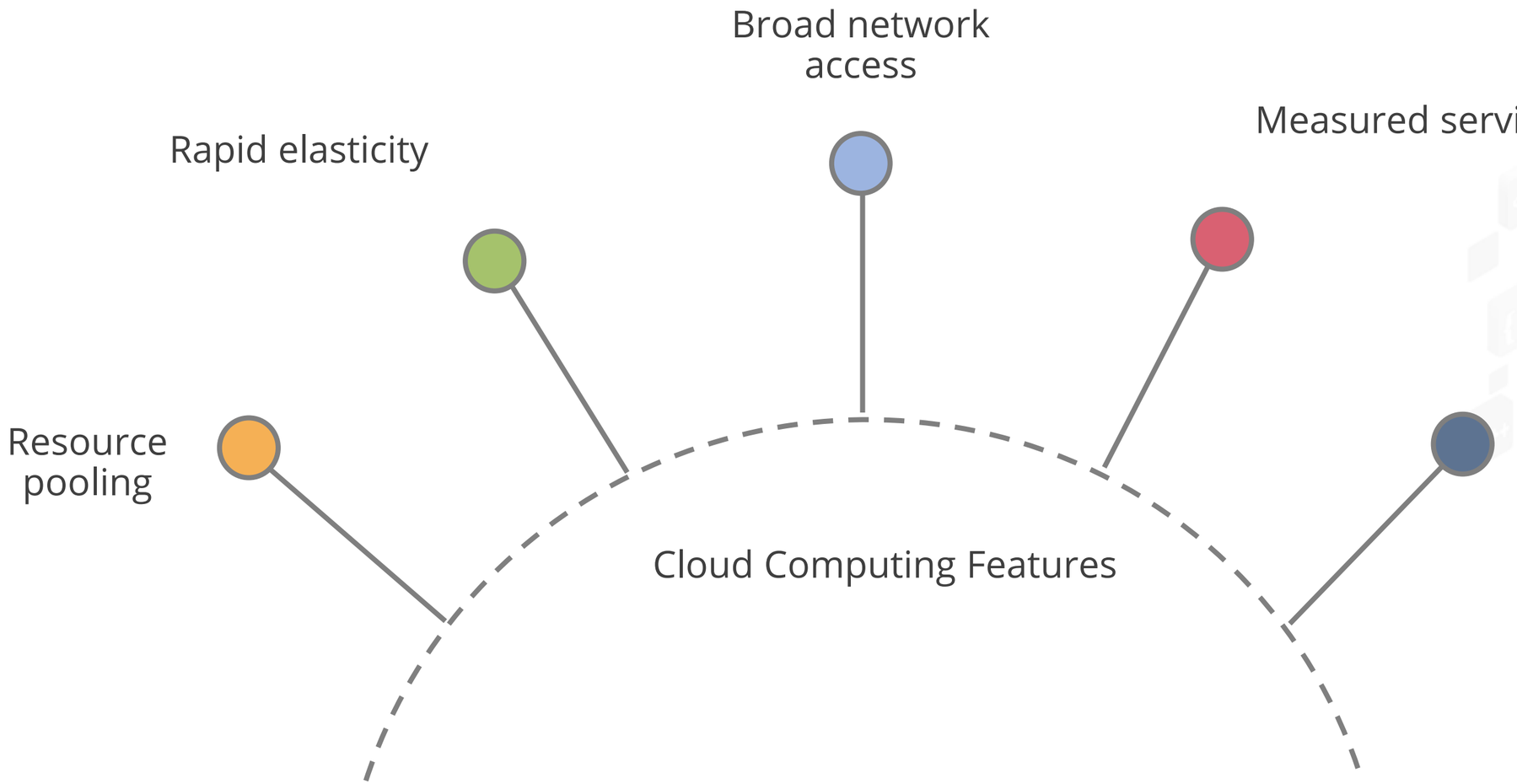
Case Study: Hypervisor Attack

This is the software code which can be installed as a thin hypervisor to control the machine under it and intercept the communication between the guest machine and the host machine.

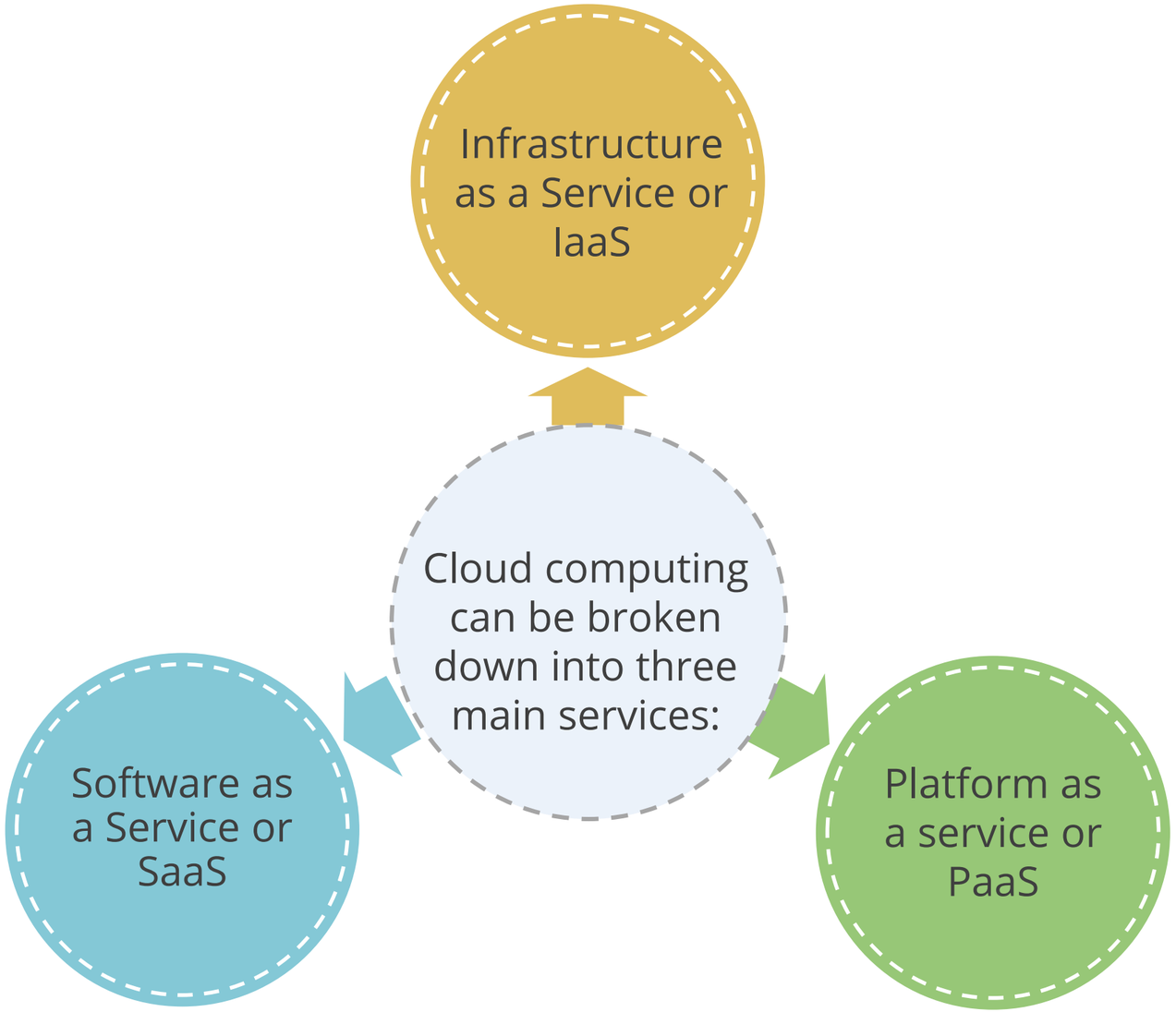
Cloud Computing

It is the use of remote servers on the internet to store, manage, and process data.

Cloud Computing Characteristics



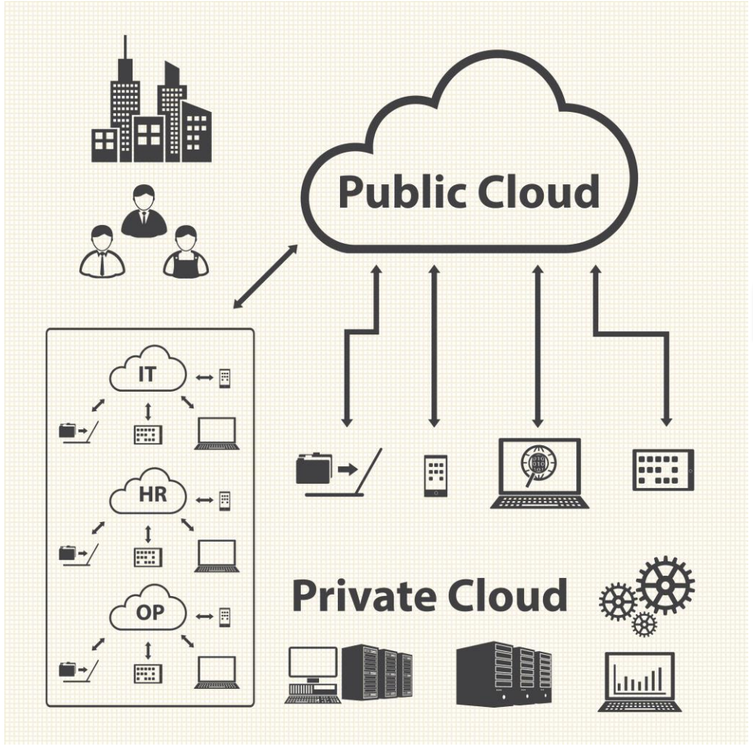
Categorization of Cloud: Service Categories



Categorization of Cloud: Deployment Categories

- Public cloud
- Private cloud
- Hybrid cloud
- Community cloud

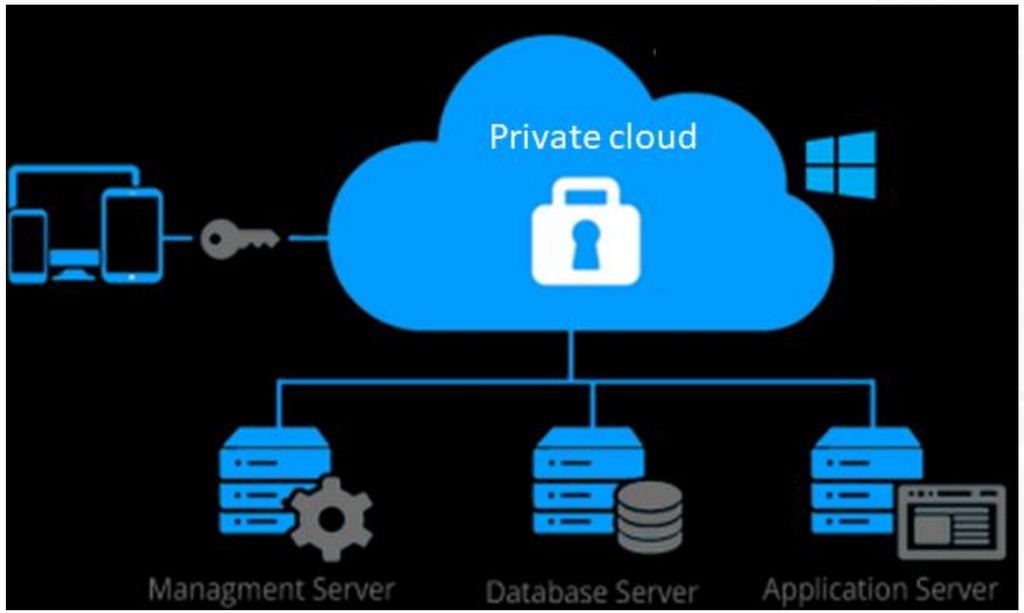
Computing infrastructure that offers cloud service



Categorization of Cloud: Deployment Categories

- Public cloud
- Private cloud
- Hybrid cloud
- Community cloud

A cloud infrastructure in an organization



Categorization of Cloud: Deployment Categories

- Public cloud
- Private cloud
- Hybrid cloud
- Community cloud

Derived from both public and private clouds

Categorization of Cloud: Deployment Categories

- Public cloud
- Private cloud
- Hybrid cloud
- Community cloud

An infrastructure between organizations to share data

Government

On premises

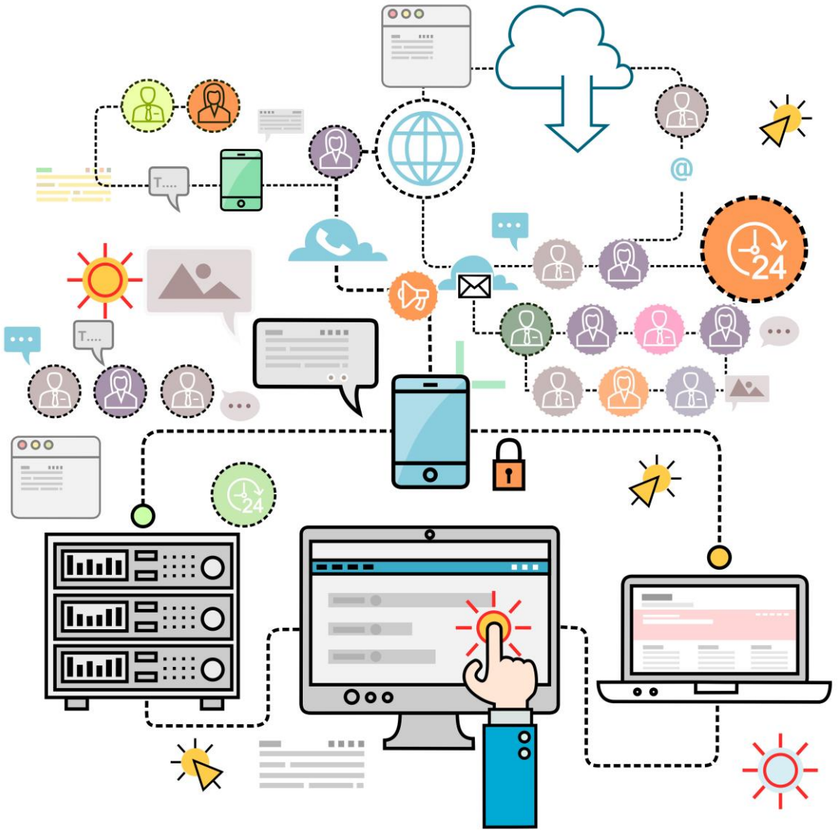
Country

Off premises

Cloud Security Challenges

Multitenancy

Privacy



Multiple jurisdiction

Virtualization complexity

Bring Your Own Device

It refers to the policy of permitting employees to bring personal devices.

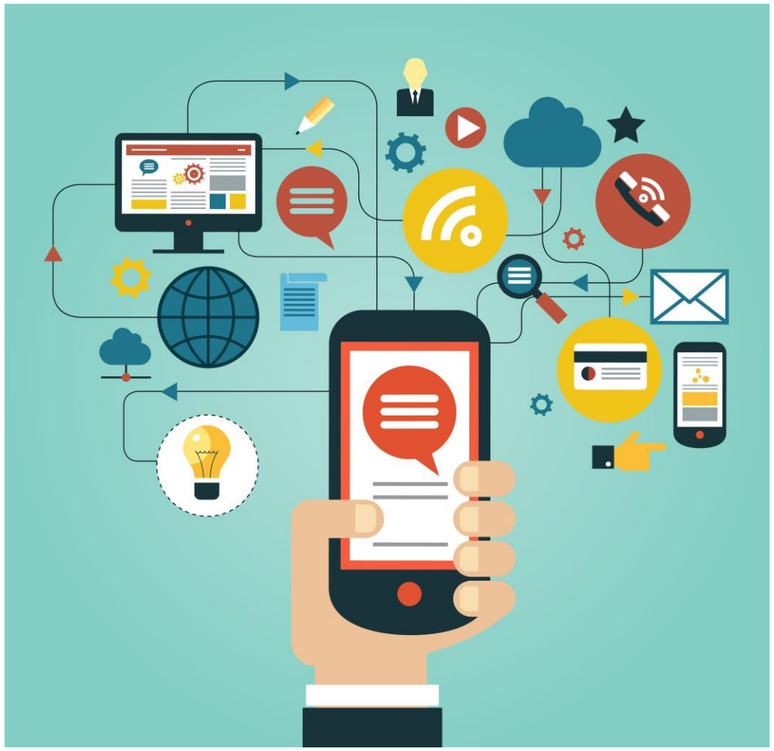
BYOT
Bring your own technology

BYOPC
Bring your own personal computer

BYOP
Bring your own phone

Bring Your Own Device: Security

It is a security software used by an IT department to monitor, manage, and secure employees' mobile devices.



Mobile Device Management

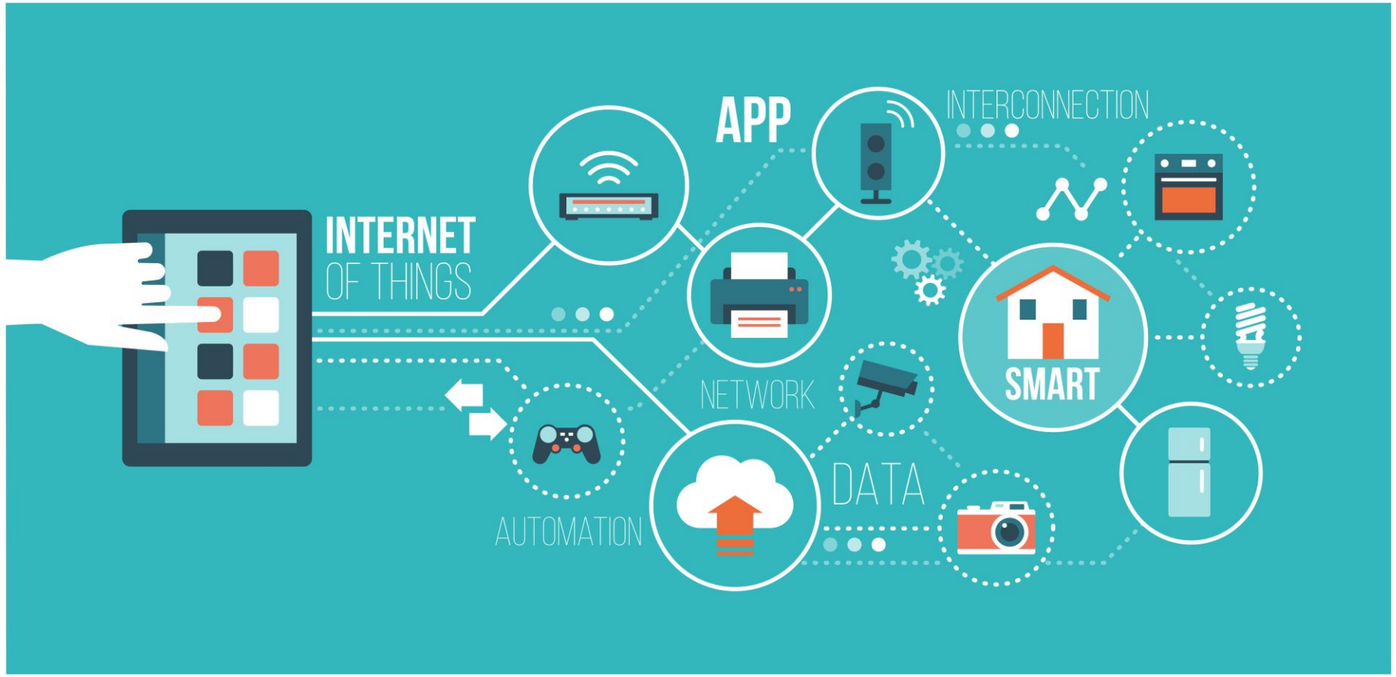
Bring Your Own Device: Security

It is similar to mobile device management. However, it manages the entire network of devices.

Enterprise Mobility Management

IoT (Internet of Things)

Internet of Things (IoT) is the network of devices that connect, interact, and exchange data.



IoT Security Challenges

Insufficient testing and updating

Brute-forcing

IoT malware and ransomware

Data security and privacy concerns

Key Takeaways

- Incident management is a process of developing and maintaining the capability of managing incidents within an organization.
- Digital forensics examines digital media with the aim of identifying, preserving, recovering, analyzing, and presenting facts and opinions about digital information.
- Business continuity deals with major disruptions, whereas disaster recovery is an organization's ability to recover from a disaster and/or unexpected events and resume operations.