ICPAK
Credibility. Professionalism. Accountability

BUSINESS CONTINUITY/DISASTER RECOVERY PLANS – A case for physical security

Date: 12th September 2019

Venue: Travelers Beach Hotel & Club - Mombasa

Presented by: CPA Hillary Wachinga

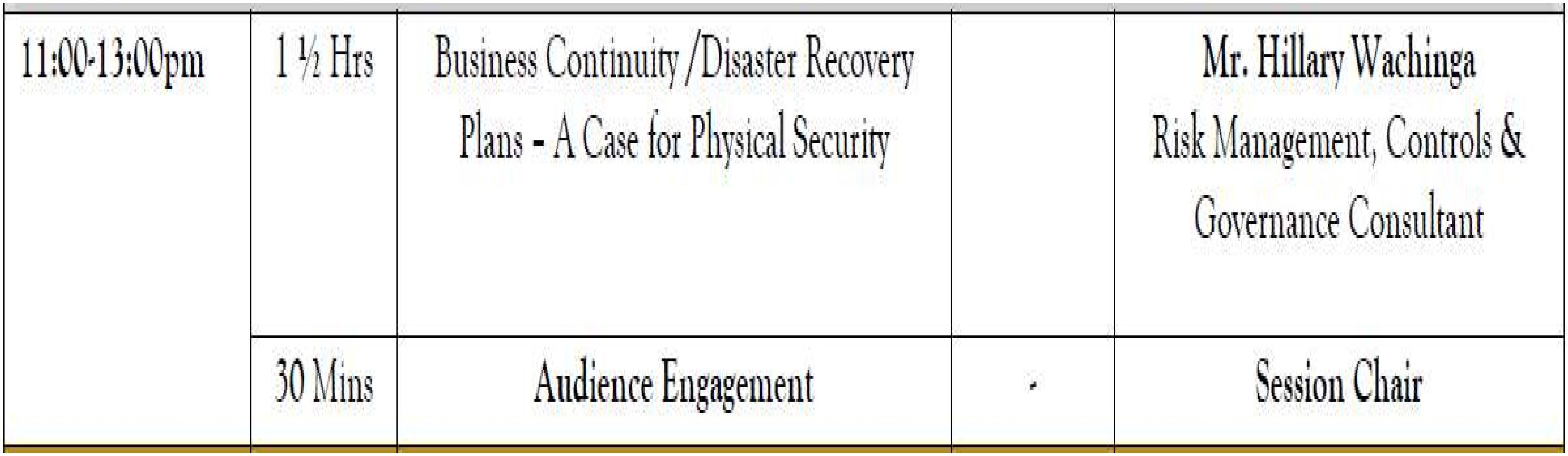
Trainer’s profile - Hillary

Hillary is an audit and risk professional with 14 years work experience gained from the Big 4, banking, insurance and reinsurance sectors.

He will graduate with a PhD (Strategic Information Systems) in December 2019. He holds masters in information systems and a BSc Computer Science. He is also a CPA(K) and has successfully passed CISA, CISA, CRISC, CISM, CCA and CERM.

He is grateful to ICPAK for the opportunity to share knowledge with its members.

Training Program



11:00-13:00pm	1 ½ Hrs	Business Continuity /Disaster Recovery Plans - A Case for Physical Security		Mr. Hillary Wachinga Risk Management, Controls & Governance Consultant
	30 Mins	Audience Engagement	-	Session Chair

Introduction

“The secret of survival is preparation”

Areas of focus

1

Business Continuity/Disaster Recovery Planning

- Introduction to BCM
- Importance of BCM
- Lifecycle of BCM
- Governance structure
- Challenges of implementing BCM
- Linking BCM and physical security

2

Physical security

- Introduction
- Physical security program
- Threat modelling
- Physical intrusion testing
- Case studies

1.0 BUSINESS CONTINUITY MANAGEMENT(BCM)

BCM can be defined as an **all-inclusive business resilience methodology** that encompasses a **framework** (policies, procedures & standards) for **making sure** that **critical** business operation(s) are **continued or restored** in a **timely manner** in case of a **disruption**.

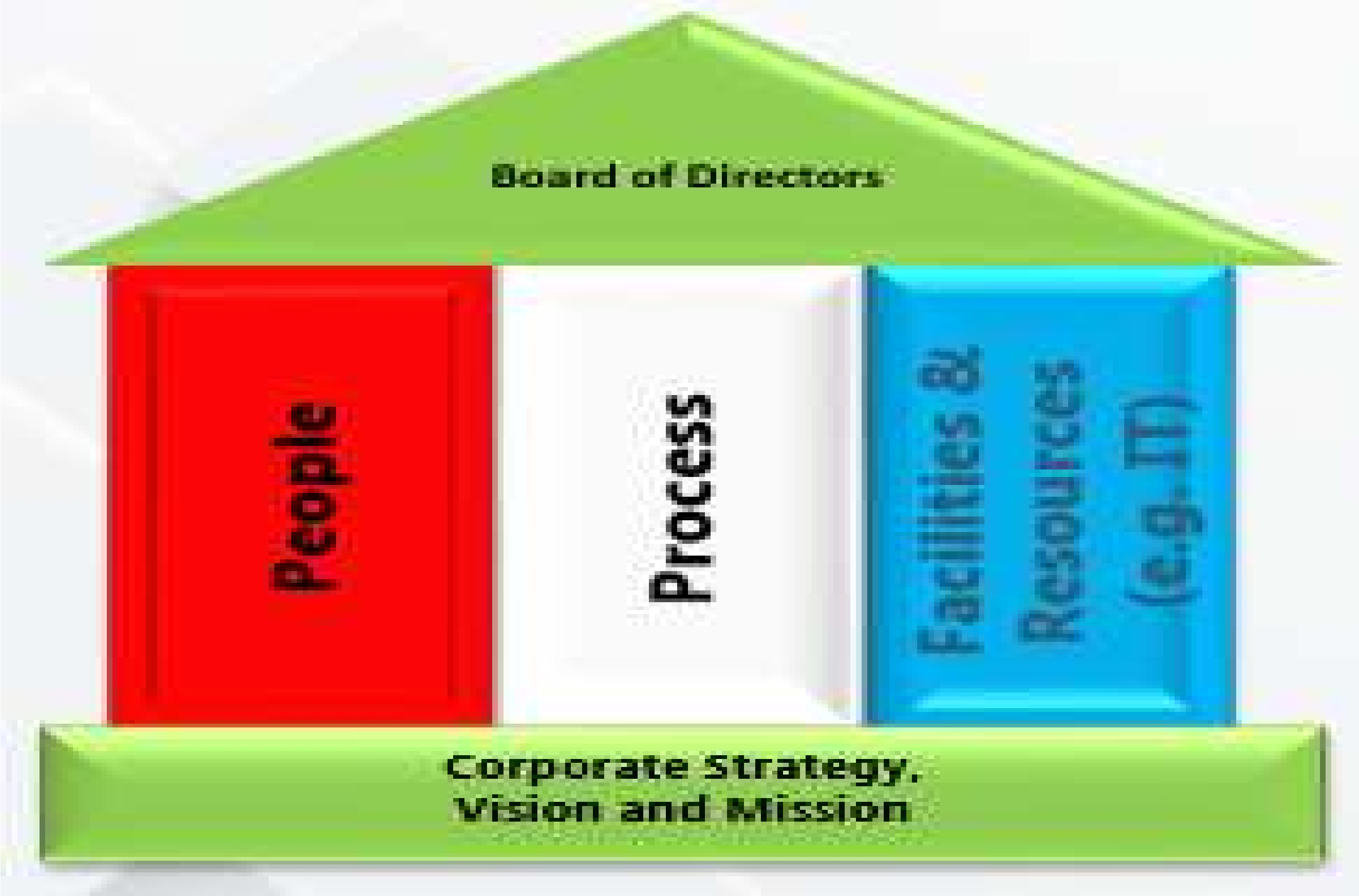
2.0 BEST PRACTICES IN BCM

a) Local key BCM regulations- Banking Act, Insurance Act, Sacco Act :

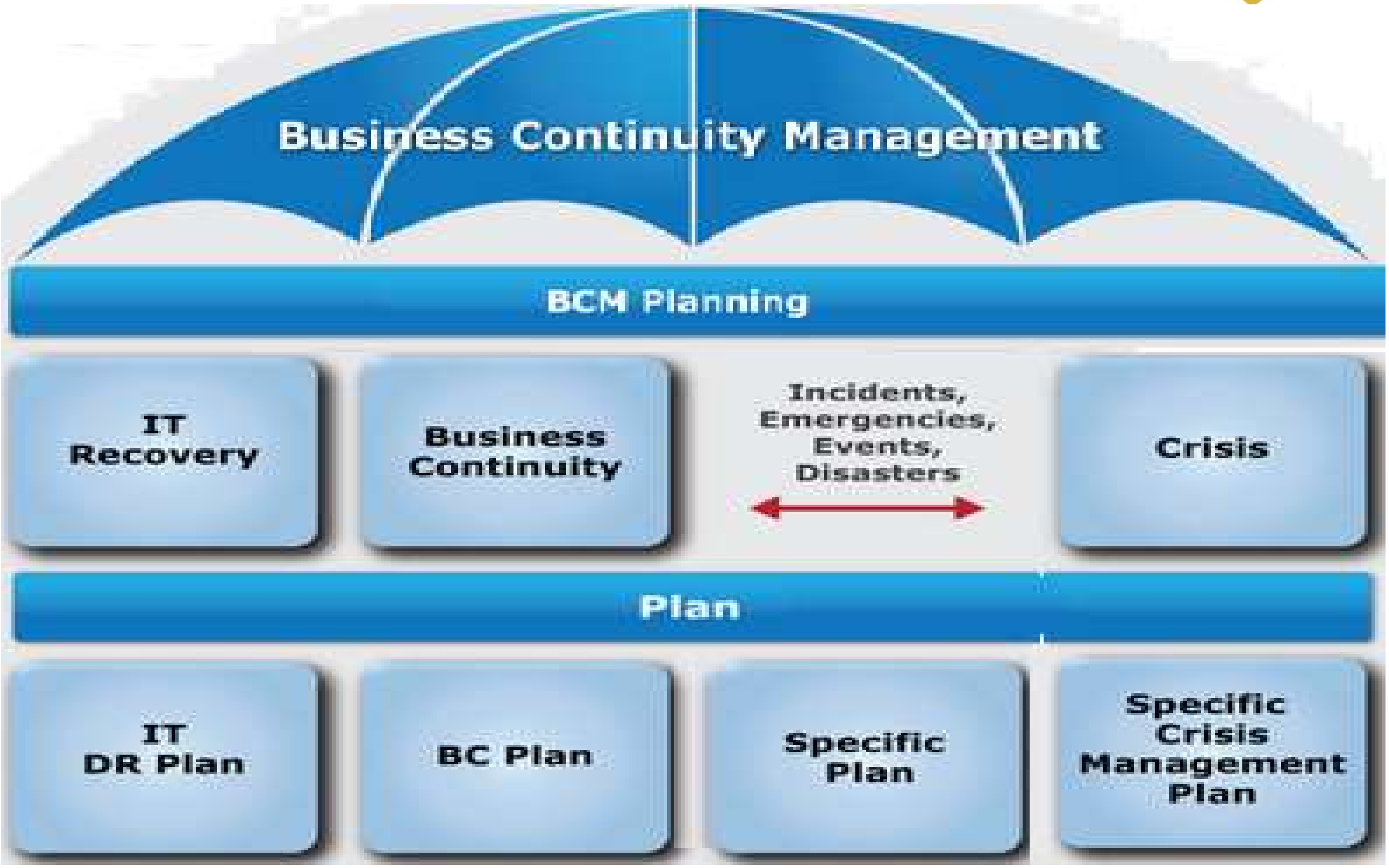
- CBK via Banking Circular No.1 of 2008 effective 1st March 2008,
- IRA Guidelines on Business Continuity Management, 2018
- SASRA Guidelines on Good Governance Practices for Deposit-Taking Saccos, July 2015

b) International: ISO 22301 (Business Continuity), ISO 28002 (Supply Chain Resilience), NIST 800, NFPA 1600 and FISMA

3.0 PILLARS OF BCM


Board of Directors
People
Process
Facilities & Resources (e.g. IT)
Corporate Strategy, Vision and Mission

4.0 BCM framework



Business Continuity Management

BCM Planning

IT Recovery

Business Continuity

Incidents, Emergencies, Events, Disasters

Crisis

Plan

IT DR Plan

BC Plan

Specific Plan

Specific Crisis Management Plan

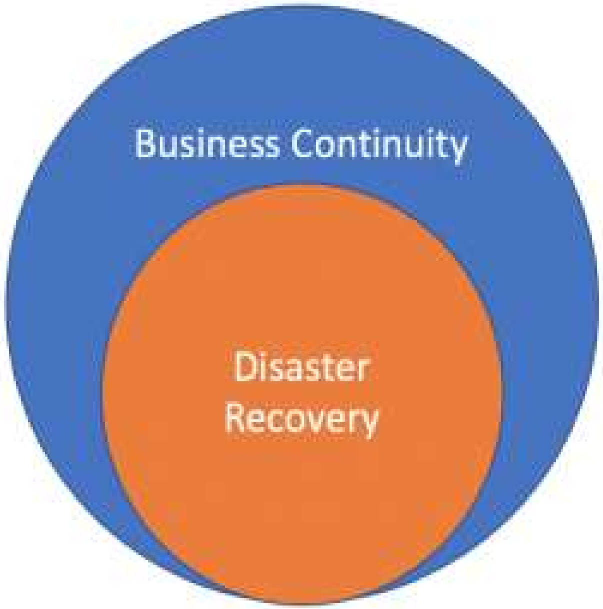
4.1 BCM framework

BCM = BCP (non-IT Ops) + DRP (IT Ops)

Where **BCP** = Business Continuity Plan

DRP = Disaster Recovery Plan

And business **disruption** => **disaster**



4.1.1 DISASTER

An unexpected/unplanned CAT event that prevents a firm from delivering its critical operations or services beyond acceptable period of time (*maximum tolerable downtime*) resulting in damage or loss beyond its tolerance levels.

❑ Natural – floods, cyclones, typhoons, earthquakes, etc

❑ Man-made – terror attacks, collapsing buildings, fires, strikes, etc

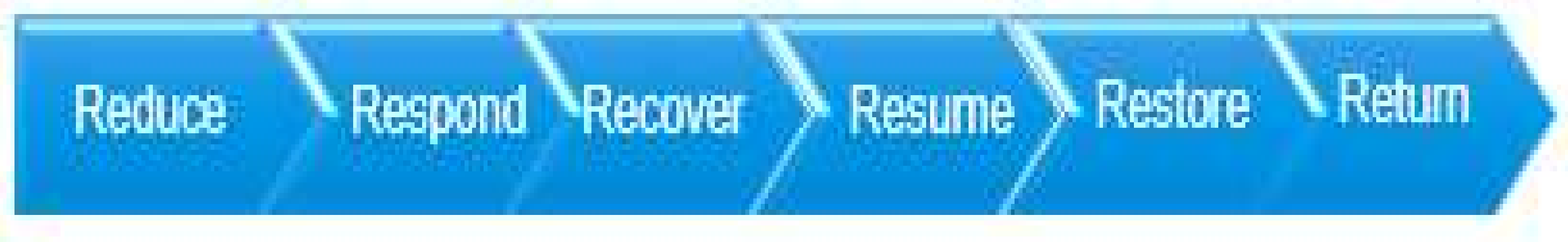
4.1.2 EXAMPLES OF DISASTERS

ICPAK

Credibility. Professionalism. Accountability

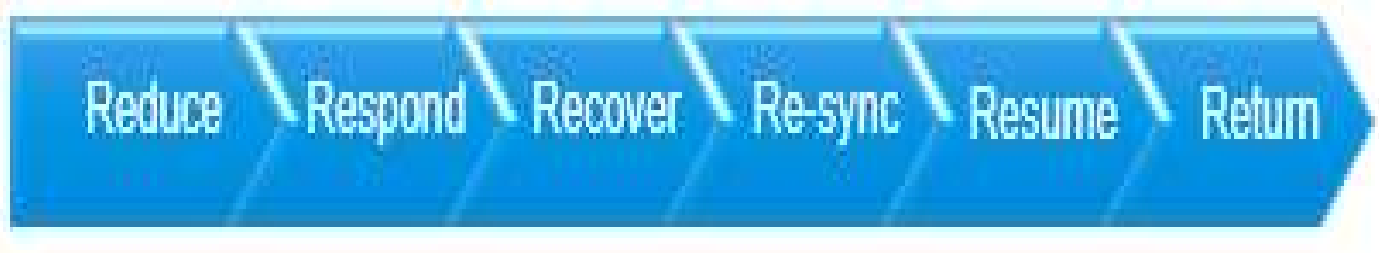
4.2 Business Continuity Plan (BCP)

BCP can be defines as a detailed **written plan of action** that **clearly indicate** procedures, processes and systems **necessary** to **continue or restore** the business operations of a firm in case of a disaster



4.3 Disaster Recovery Planning

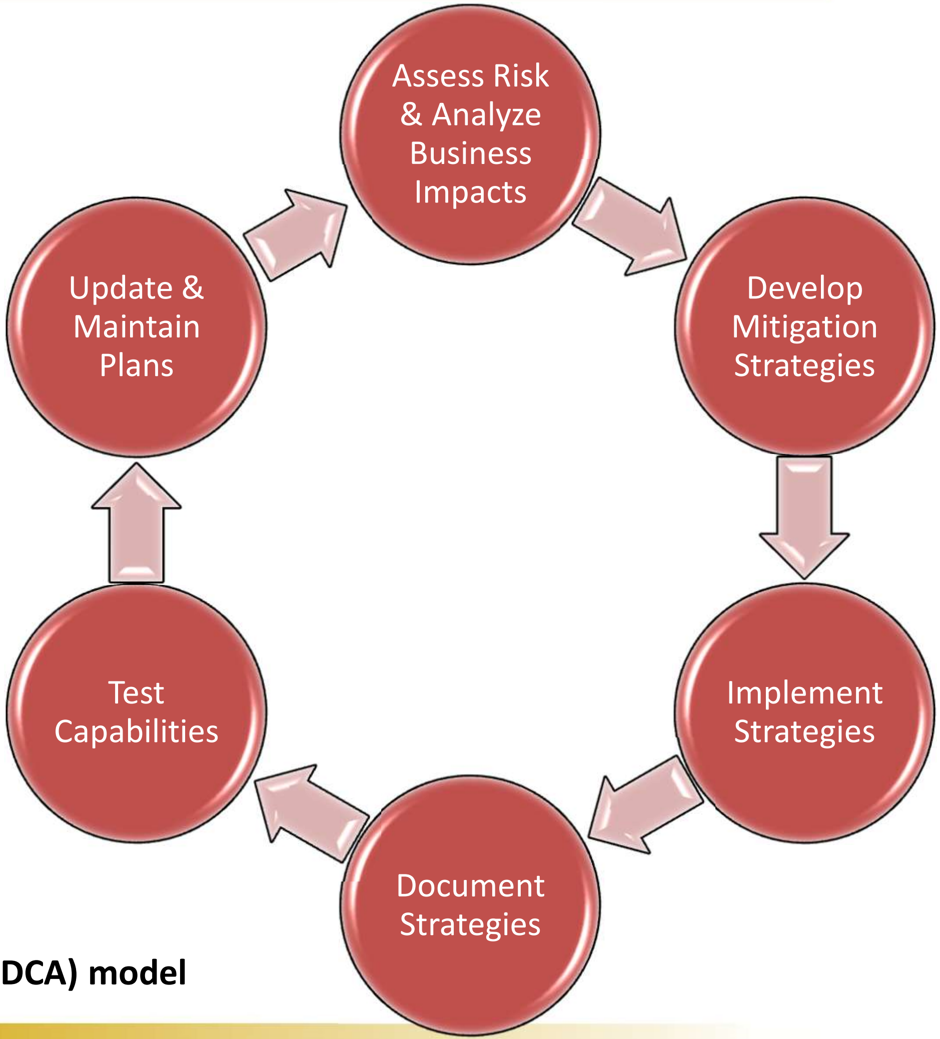
DRP is a framework (policies, procedures, tools) to ensure continuation or restoration of critical IT resources (infrastructure, applications, etc) for predetermined time after a disaster.



5.0 Importance of BCM

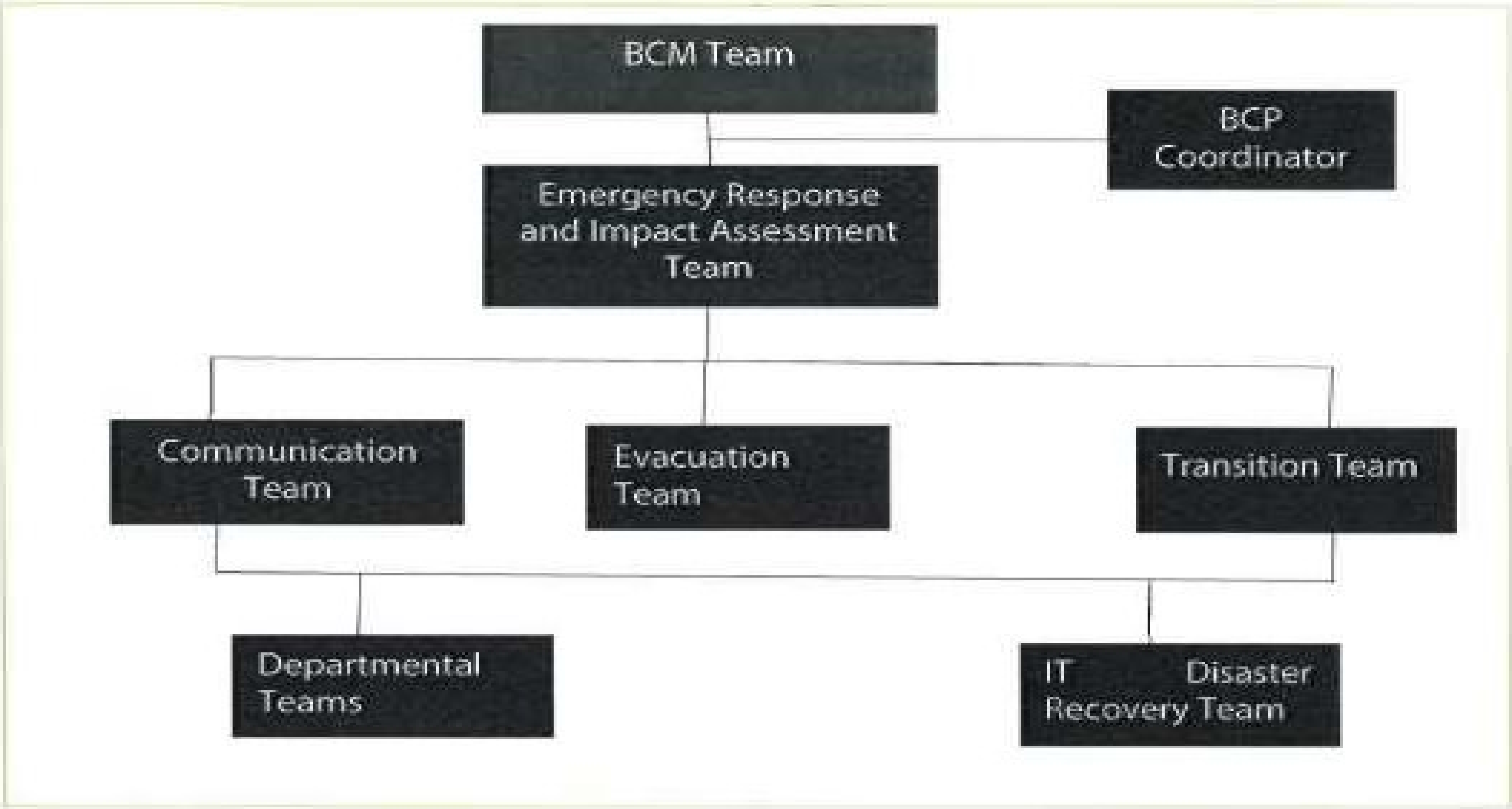
- ❑ Increases competitive advantage
- ❑ Improves stakeholders confidence and brand value
- ❑ Reduces costs – legal suits, insurance premiums, capital, etc
- ❑ Creates resilience in business and IT operations – assist business in meeting its obligations with minimal disruption
- ❑ Compliance to regulatory requirements

6.0 Lifecycle of BCM



Based on Plan-Do-Check-Act (PDCA) model

7.0 Governance structure of a BCM



BCM Team

BCP Coordinator

Emergency Response and Impact Assessment Team

Communication Team

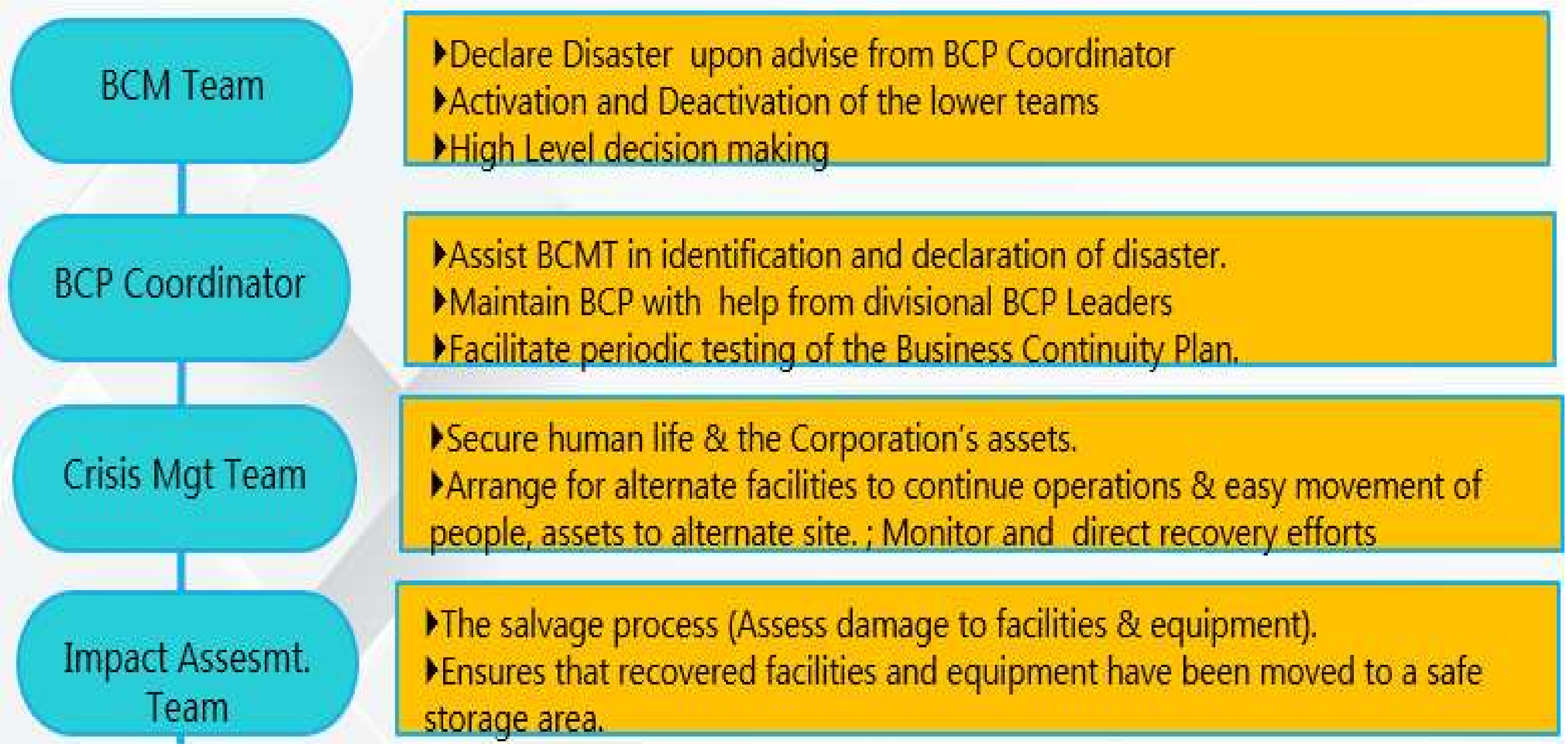
Evacuation Team

Transition Team

Departmental Teams

IT Disaster Recovery Team

7.1 Roles in a BCM structure



BCM Team

- Declare Disaster upon advise from BCP Coordinator
- Activation and Deactivation of the lower teams
- High Level decision making

BCP Coordinator

- Assist BCMT in identification and declaration of disaster.
- Maintain BCP with help from divisional BCP Leaders
- Facilitate periodic testing of the Business Continuity Plan.

Crisis Mgt Team

- Secure human life & the Corporation's assets.
- Arrange for alternate facilities to continue operations & easy movement of people, assets to alternate site. ; Monitor and direct recovery efforts

Impact Assesmt. Team

- The salvage process (Assess damage to facilities & equipment).
- Ensures that recovered facilities and equipment have been moved to a safe storage area.

7.2.1 BCM teams

TEAM	RESPONSIBILITIES
Emergency Response & Impact Assessment Team	The team manages all activities during and after a disaster until declaration of normalization of business. This is by coordinating the activities of the other BCM teams
Impact Assessment Team	The team is responsible for securing assets of the Corporation at the disaster site.
Evacuation / Emergency Support Team	They is responsible for securing human life.
Communication Team	The team is responsible for facilitating communication with both internal and external stakeholders.
Transition Team	The team is responsible for effectively planning, coordinating and executing logistics involved in movement of people and equipment during the disaster and restoration period.

7.2.2 BCM teams

IT Disaster Recovery Team

This team shall largely comprise members of the ICT Division. They shall be responsible for identifying and ensuring that critical IT resources and the data centre are restored to facilitate resumption of operations.

These resources include:

i) Hardware Resources

ii) Software Resources

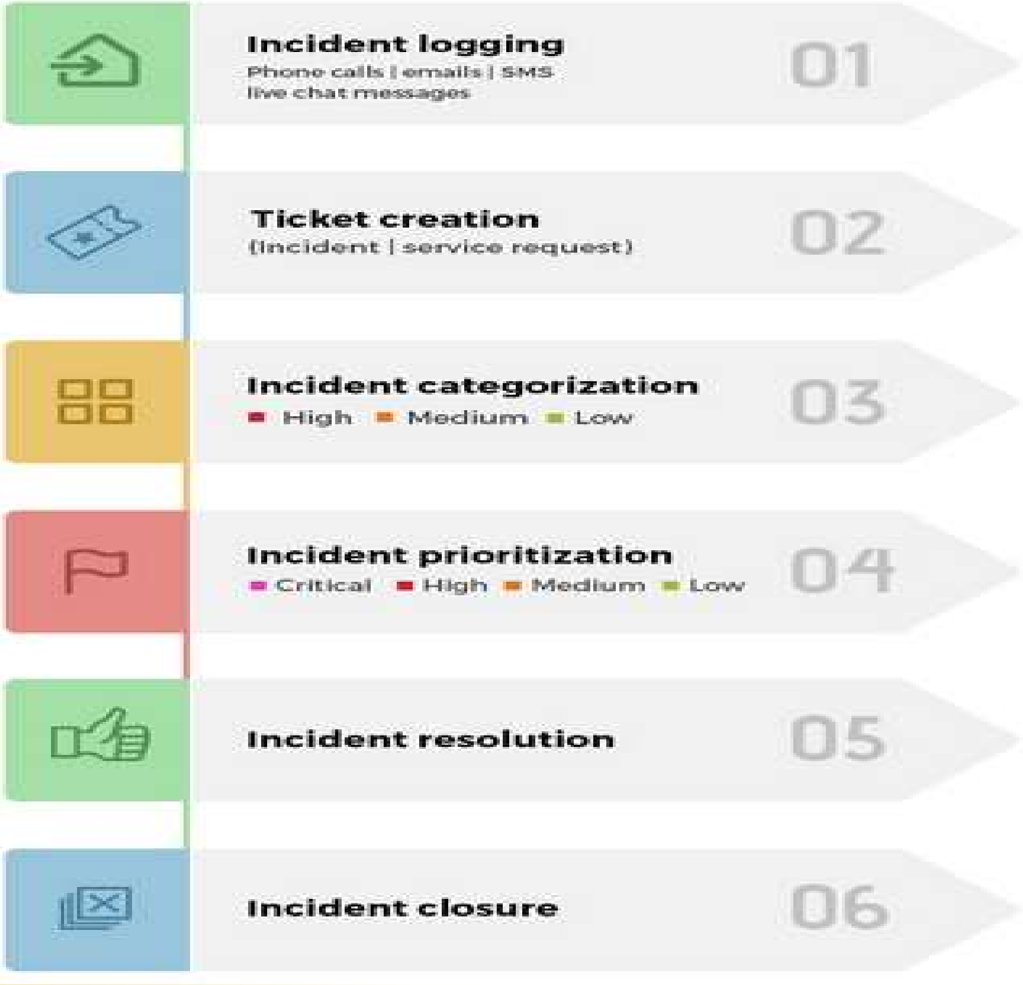
iii) Network requirements

8.0 Challenges in implementation of a BCM

- ❑ Inadequate integration between risk management and BCM
- ❑ Poor resourcing – monetary and human capital
- ❑ Rapid changes in business environment, especially changes in technology
- ❑ Increasing expectations from regulators and other stakeholders on minimal disruption and loss of data
- ❑ Lack of support by management – not prepared, BCM not tested
- ❑ 3rd Party supplier risk

9.0 Linking BCM and physical security

- ❑ Via **incident management:**



Incident logging 01
Phone calls | emails | SMS
live chat messages

Ticket creation 02
(Incident | service request)

Incident categorization 03
■ High ■ Medium ■ Low

Incident prioritization 04
■ Critical ■ High ■ Medium ■ Low

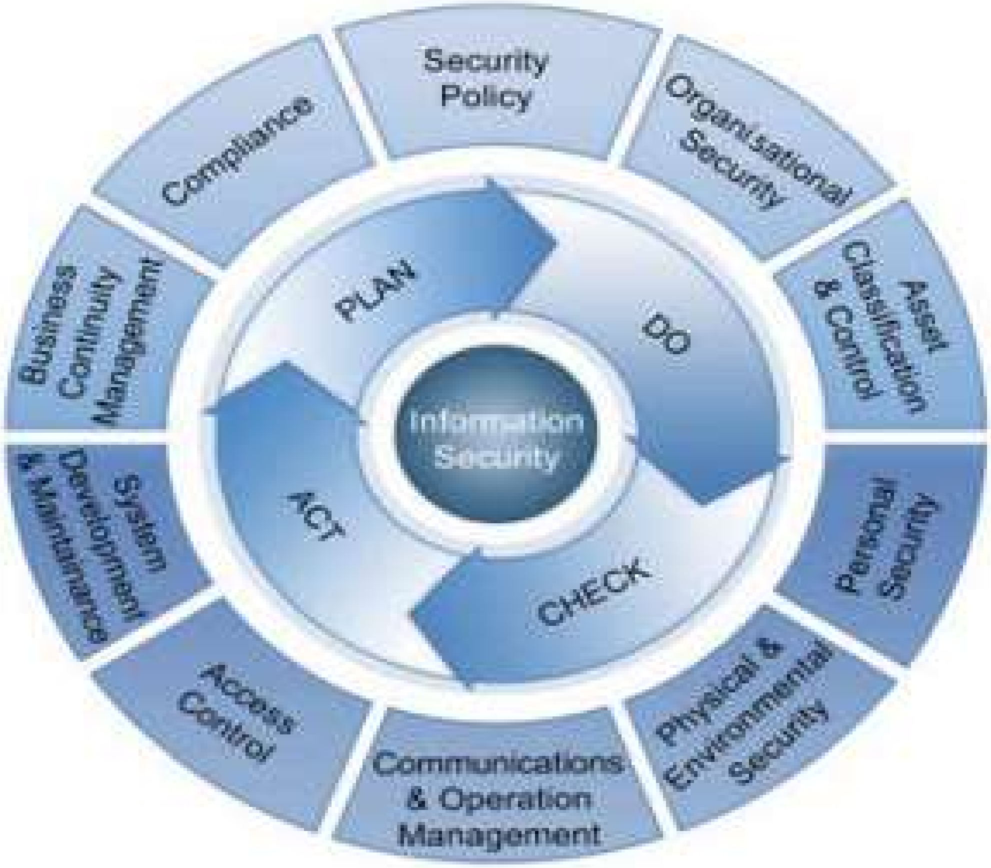
Incident resolution 05

Incident closure 06

9.0 Linking BCM and physical security

❑ **Incident management:** - aimed at enhancing physical security

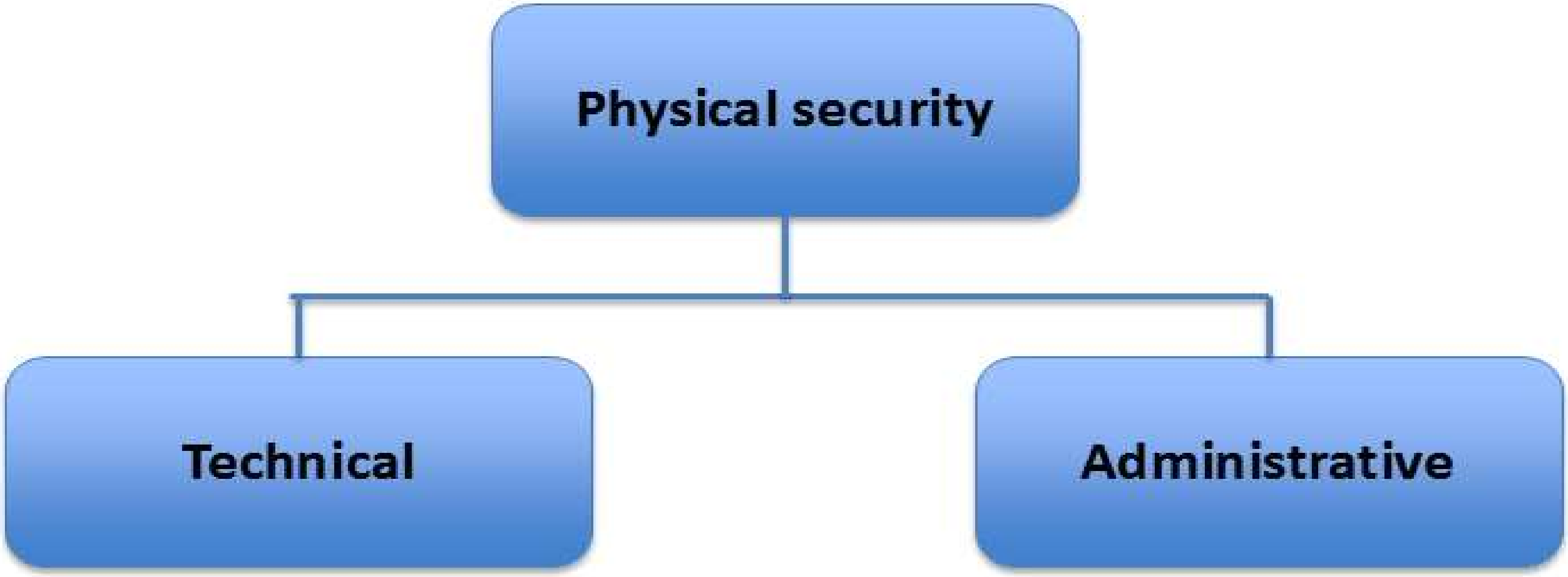
❑ ISO 27001


Security Policy
Organisational Security
Asset Classification & Control
Personal Security
Physical & Environmental Security
Communications & Operation Management
Access Control
System Development & Maintainance
Business Continuity Management
Compliance
PLAN
DO
CHECK
ACT
Information Security

Credibility . Professionalism . Accountability

PHYSICAL SECURITY

1.0 Elements of Physical Security



NB: Most firms concentrate on “technology-oriented security countermeasures” in safeguarding their information assets.

2.0 Aim of Physical Security

- "***objective of physical security is to safeguard personnel, information, equipment, IT infrastructure, facilities and all other company assets***" - SAN Institute
- Treated as an after-thought in information security. Given least focus by management

3.0 Why Physical Security

- ❑ Advent of portable data storage devices – increasing likelihood of losing lots of data when such devices get lost or are stolen.
- ❑ Increased threats – fraud/collusion, sabotage, theft, vandalism, etc
- ❑ Stakeholders expectations that a firm must safeguard its information assets – regulators, shareholders, 3rd parties
- ❑ Increased legal risk incase of damage arising from breach of physical security.
- ❑ Risk mitigation – readiness, reduction of casualties

4.0 Measures for physical security

- ❑ **Preventative**

  ✓Purposed to restrict access

  ✓Includes deterrent measures

  ✓E.g. smart access control card systems, security guards, trap doors, cable locks, RFID, gates,fences, etc

- ❑ **Restorative**

  ✓Purposed to restore system status incase preventative measures fail

  ✓They are detective and minimize damage

  ✓E.g. smart access control card systems, Security cameras (CCTV & IP cameras), access logs, etc

5.0 Components of physical security program

i. Site design & layout

ii. Environmental scanning

iii. Emergency response readiness

iv. Training

v. Intrusion detection

vi. Power & fire protection

5.1 Considerations in developing physical security program

i. Based on Plan-Do-Check-Audit model

ii. Multi-layered design to make it difficult to bypass – “***defense in depth***”

iii. Strike balance between security measures, safety concerns and business needs/operations (alignment)

iv. Hardening of controls - administrative, technical and physical controls.

v. Informed by principles of confidentiality, integrity and availability of information assets (priority being safeguarding human life)

vi. Proper governance structure (M&E) and resourcing

5.1.1 Example of layers of physical security

- ❑ **Ground entrance -** Security guards, gates & fences
- ❑ **Building entrance -** Security guards, employee/ID badge
- ❑ **Individual office/room entrance -** Biometric scanners, proximity cards, ID badge
- ❑ **Personal belongings -** Lock & key for PCs/laptops/servers, safes for backups
- ❑ **Multiple-layered security –e.g. military barracks**

5.2 Evaluating effectiveness of a physical security program

i. Align business objectives of the program to corporate objectives

ii. Set clearly defined KPIs for the physical security program e.g.

- ✓ No. of successful disruptions
- ✓ No. of unsuccessful disruptions
- ✓ Time between detection of a security breach, assessment and recovery
- ✓ No. of false positive detection alerts
- ✓ Financial loss of a successful security breach

iii. Monitor and evaluate performance against set KPIs on pre-agreed frequencies – quarterly, semi-annually, annually, etc

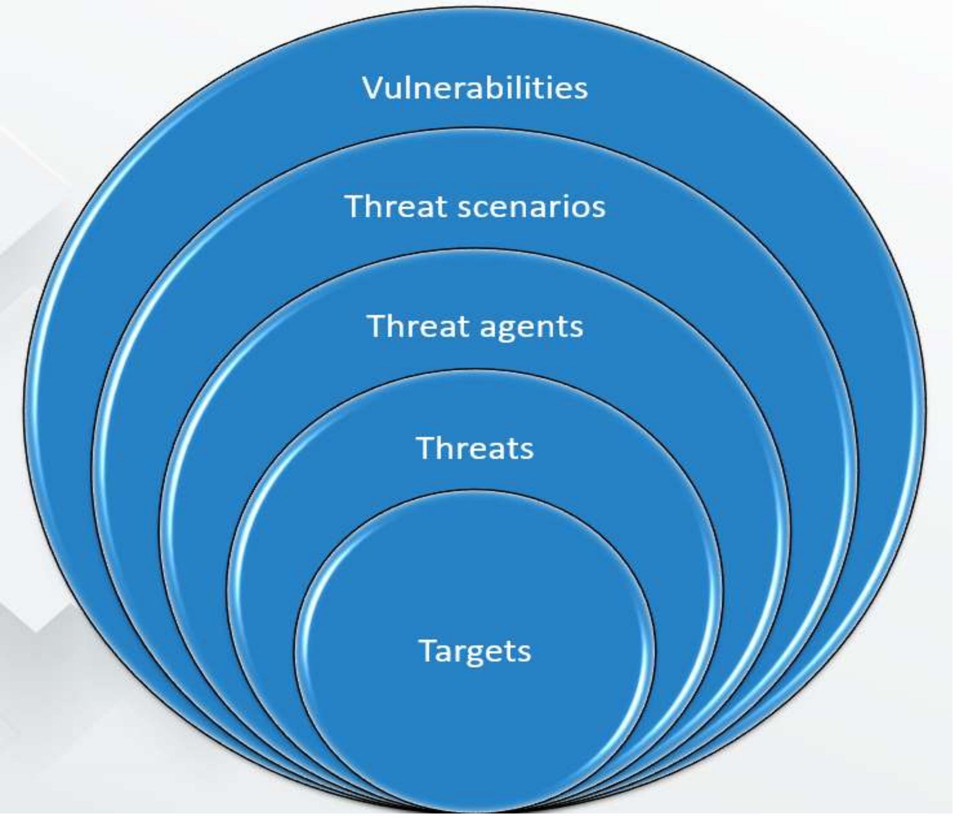
6.0 Physical security threat modelling

i. Threat profiling

ii. Risk assessment

iii. Performance against baselines

iv. Mitigation


Vulnerabilities

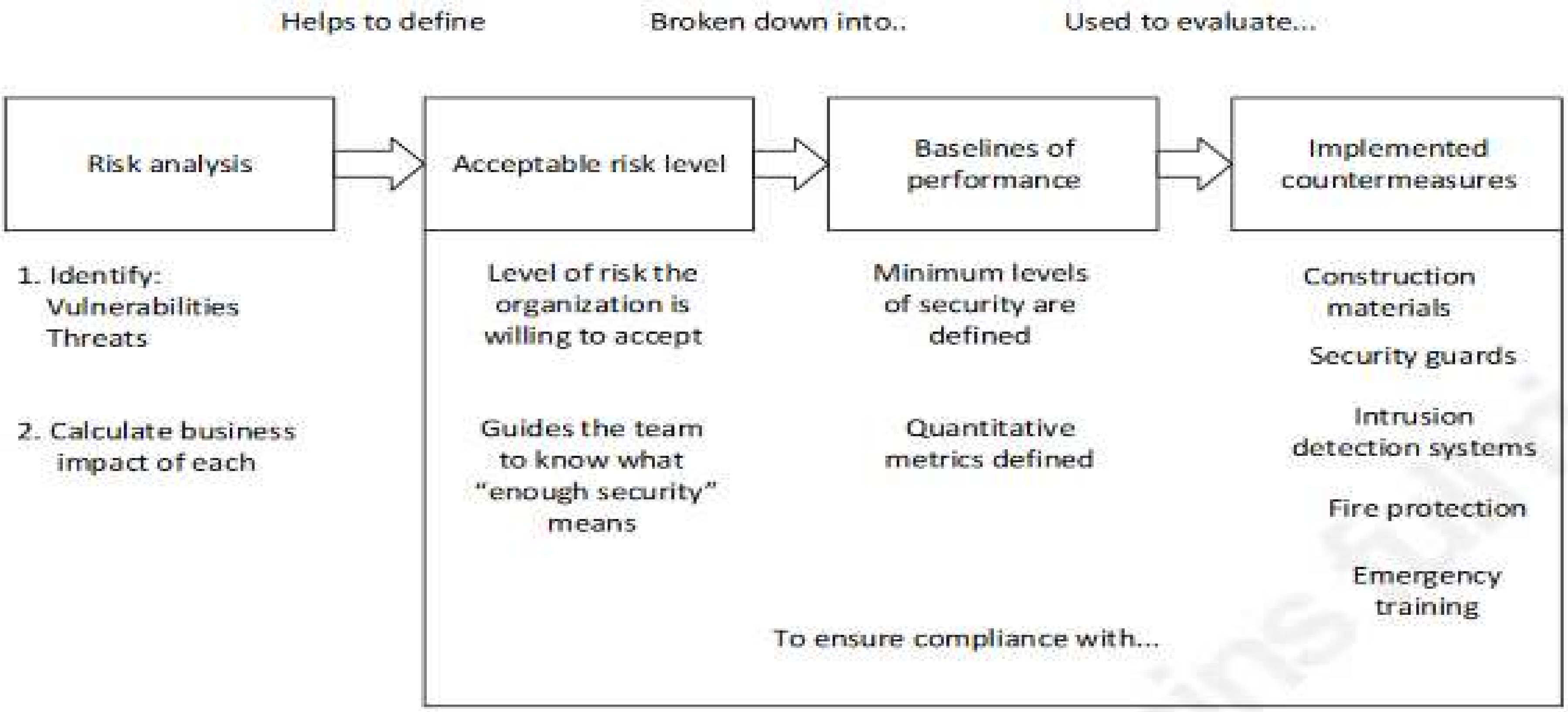
Threat scenarios

Threat agents

Threats

Targets

6.1 Physical security threat modelling



Helps to define

Broken down into..

Used to evaluate...

Risk analysis

1. Identify:
   Vulnerabilities
   Threats

2. Calculate business impact of each

Acceptable risk level

Level of risk the organization is willing to accept

Guides the team to know what "enough security" means

Baselines of performance

Minimum levels of security are defined

Quantitative metrics defined

Implemented countermeasures

Construction materials

Security guards

Intrusion detection systems

Fire protection

Emergency training

To ensure compliance with...

Relationships of risk, baselines and countermeasures Harris, (2013)

6.2 Threats to physical security

- ❑ **Tailgating attack** – also “**piggybacking**”, where unauthorized person closely follows/impersonates an authorized personnel to gain access to restricted area.
- ❑ Forceful physical access through breakage
- ❑ Theft of access control smart cards or using stolen details of such cards to gain access.
- ❑ Outage of power or physical security system
- ❑ Collusion/fraud

6.2.1 Case studies

❑ In 2014 alone, approx 74,000 employees, suppliers, and contractors were affected by a data breach because of stolen laptops with unencrypted personal data

❑ An ex-staff of Coca-Cola filed a class action lawsuit against the firm claiming it was “negligent in securing personal data”

❑ In 2008, an employee of U.S. Department of Defense base in the Middle East inserted an infected USB into the military laptop. The virus spread undetected in both unclassified and classified government systems and sent data back to remote servers in other countries

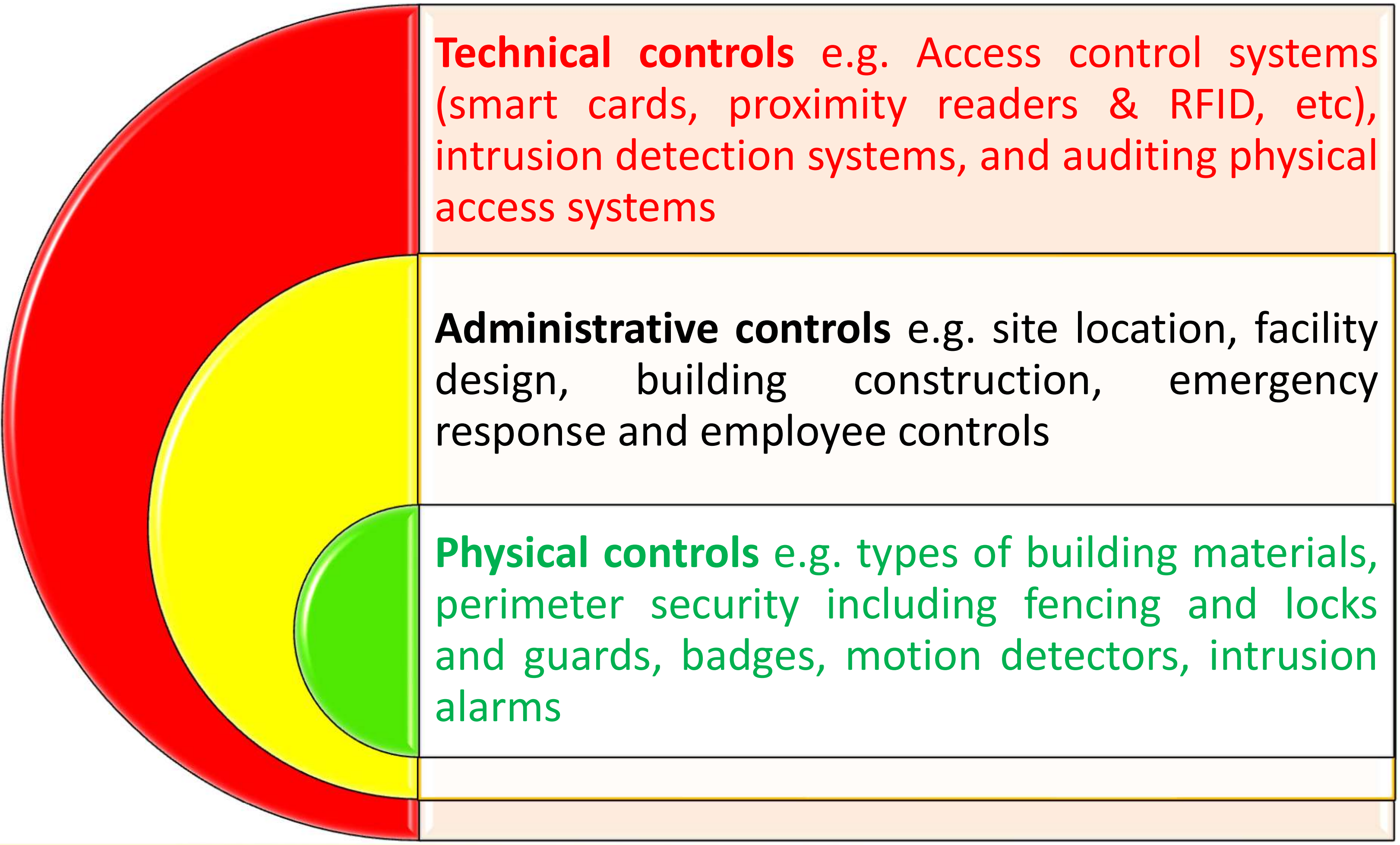
6.3 Mitigation against physical security threats

- ❑ Background checks/clearance/screening
- ❑ Polygraph tests
- ❑ Staff rotations
- ❑ Segregation of roles
- ❑ Physical security audits - on effectiveness of **physical security controls**

Physical security controls

6.3.1 Physical security controls

Consists of:



Technical controls e.g. Access control systems (smart cards, proximity readers & RFID, etc), intrusion detection systems, and auditing physical access systems

Administrative controls e.g. site location, facility design, building construction, emergency response and employee controls

Physical controls e.g. types of building materials, perimeter security including fencing and locks and guards, badges, motion detectors, intrusion alarms

6.3.2 Enhancing physical security controls

- **Principle of least privilege (POLP) -** limiting

User access rights limited to the bare

minimum permissions needed to

perform tasks.

- **Physical penetration testing**

- **Combined effort –** physical &

logical security involving all staff

6.3.3 Physical penetration testing - objectives

- ❑ Testing operating effectiveness and efficiency of physical security controls in safeguarding information assets.
- ❑ Also called physical intrusion testing
- ❑ Identify weakness of the physical security program that can lead to data breaches and compromise of information security.
- ❑ Simulate real attack situation
- ❑ Assist in strengthening physical security

6.3.3 Physical penetration testing - scope

Multi-layered security system

- ❑ Physical barriers
- ❑ Security guards
- ❑ Situational awareness
- ❑ Doors and locks
- ❑ Sensors, alarms and cameras
- ❑ biometrics

6.3.3 Physical penetration testing - tests

May involve conducting the following checks

- ❑ Character impersonification/tailgating
- ❑ Door bypass and lock picking
- ❑ ID or badge cloning
- ❑ Onsite reconnaissance
- ❑ Covert (*unaware*) and overt (*fully aware*) operations

6.3.3 Physical penetration testing - tools

Some of the most preferred tools for physical intrusion testing:

- ❑ Open Source Intelligence (OSINT)
- ❑ Active reconnaissance (use of drones, satellites, etc)
- ❑ Passive reconnaissance – gather info without actively engaging target
- ❑ Exploitation
- ❑ Vulnerability assessment

6.3.3 Case studies

□ **Physical penetration testing: https://www.youtube.com/watch?v=P4HIDJ-5lJo**

□ **https://www.youtube.com/watch?v=EXrxtHWKs6Q**

Q & A