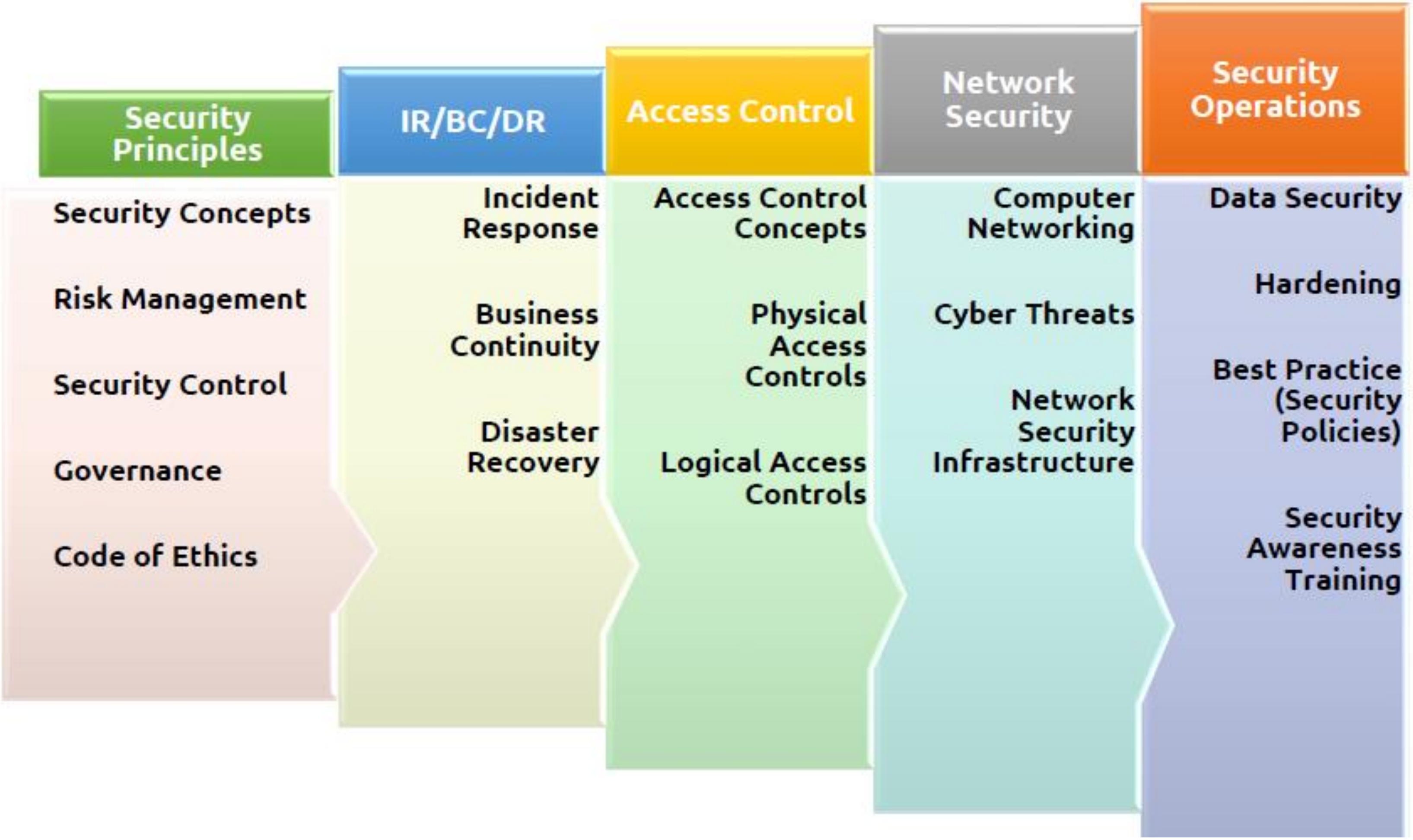
ISC2 CC Exam – Last min. Review



Security Principles

- Security Concepts
- Risk Management
- Security Control
- Governance
- Code of Ethics

IR/BC/DR

- Incident Response
- Business Continuity
- Disaster Recovery

Access Control

- Access Control Concepts
- Physical Access Controls
- Logical Access Controls

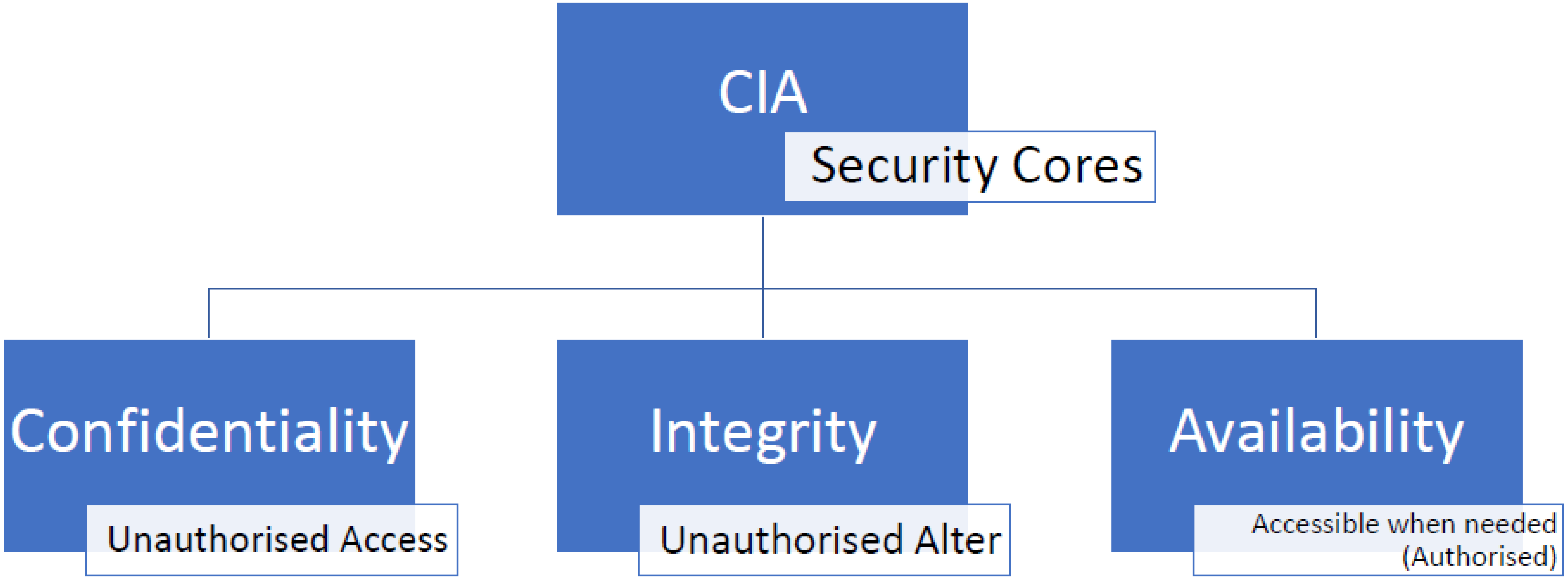
Network Security

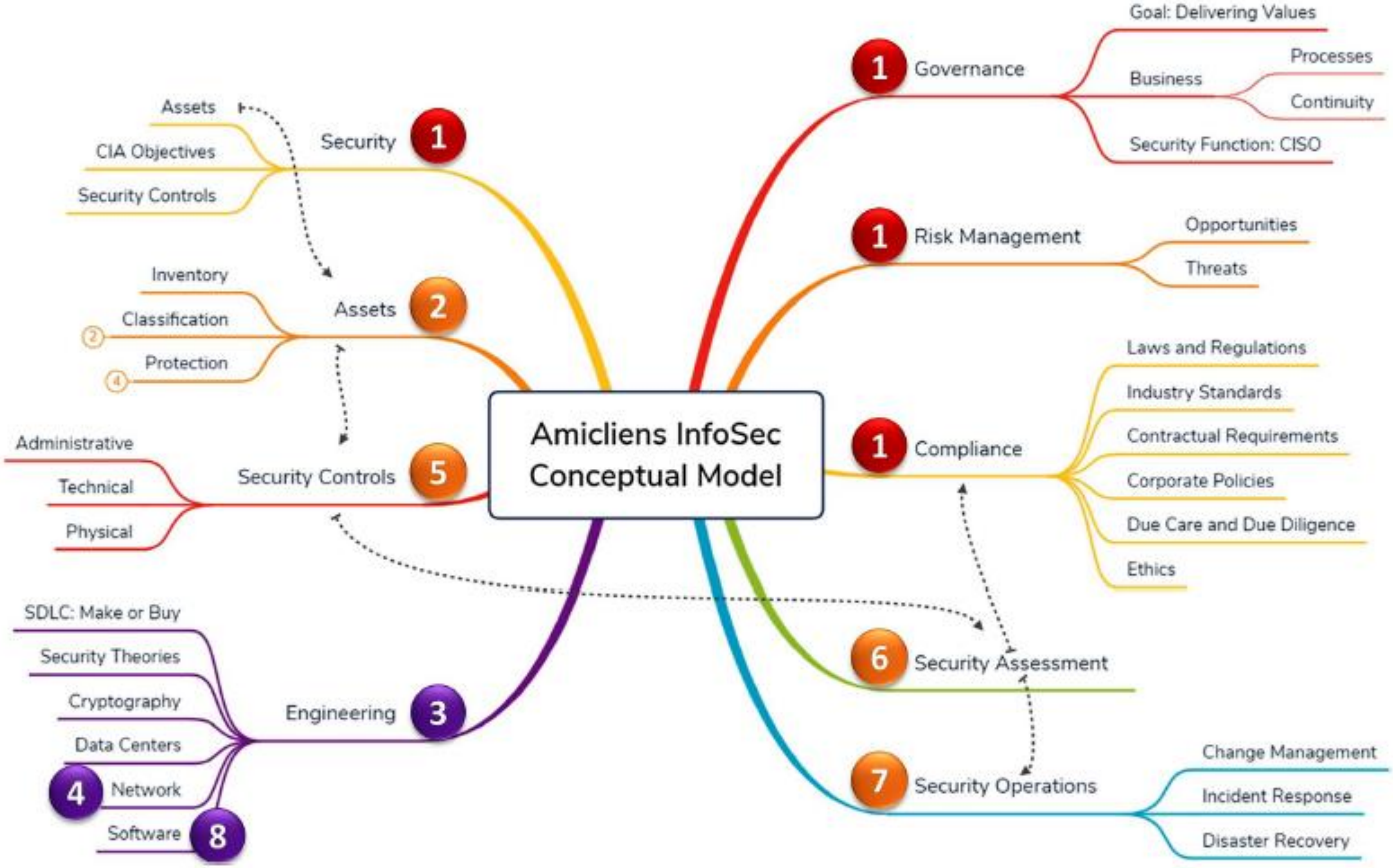
- Computer Networking
- Cyber Threats
- Network Security Infrastructure

Security Operations

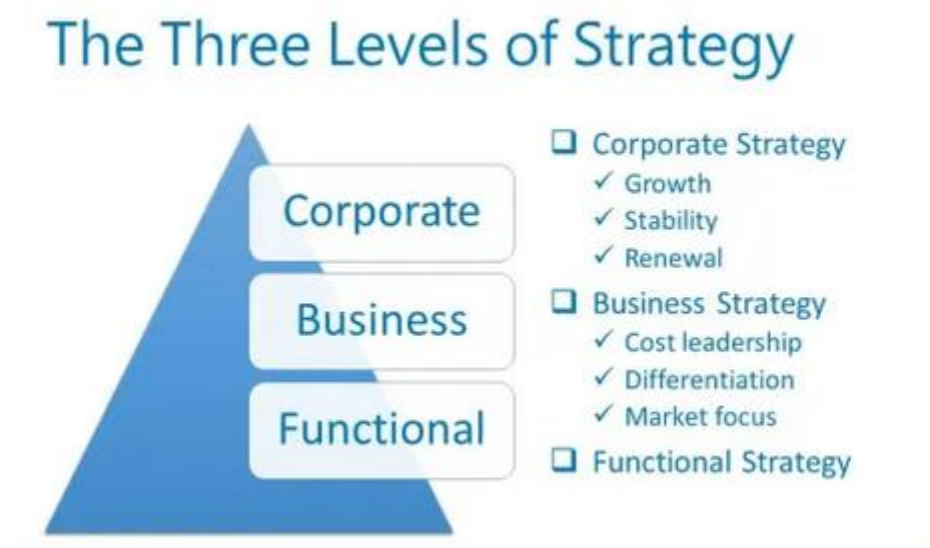
- Data Security
- Hardening
- Best Practice (Security Policies)
- Security Awareness Training

Security Principles



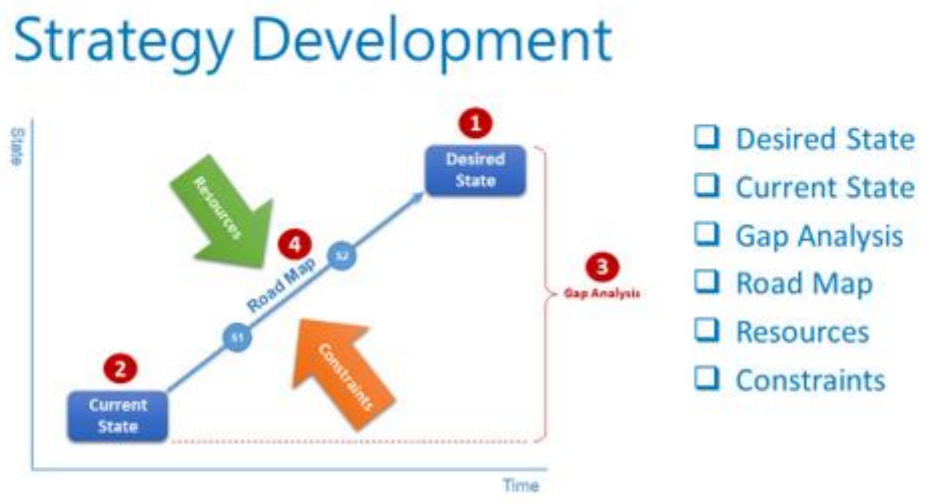


Amicliens InfoSec Conceptual Model
Security 1
Assets
CIA Objectives
Security Controls
Assets 2
Inventory
Classification
2
Protection
4
Security Controls 5
Administrative
Technical
Physical
Engineering 3
SDLC: Make or Buy
Security Theories
Cryptography
Data Centers
4 Network
Software 8
1 Governance
Goal: Delivering Values
Business
Processes
Continuity
Security Function: CISO
1 Risk Management
Opportunities
Threats
1 Compliance
Laws and Regulations
Industry Standards
Contractual Requirements
Corporate Policies
Due Care and Due Diligence
Ethics
6 Security Assessment
7 Security Operations
Change Management
Incident Response
Disaster Recovery



The Three Levels of Strategy

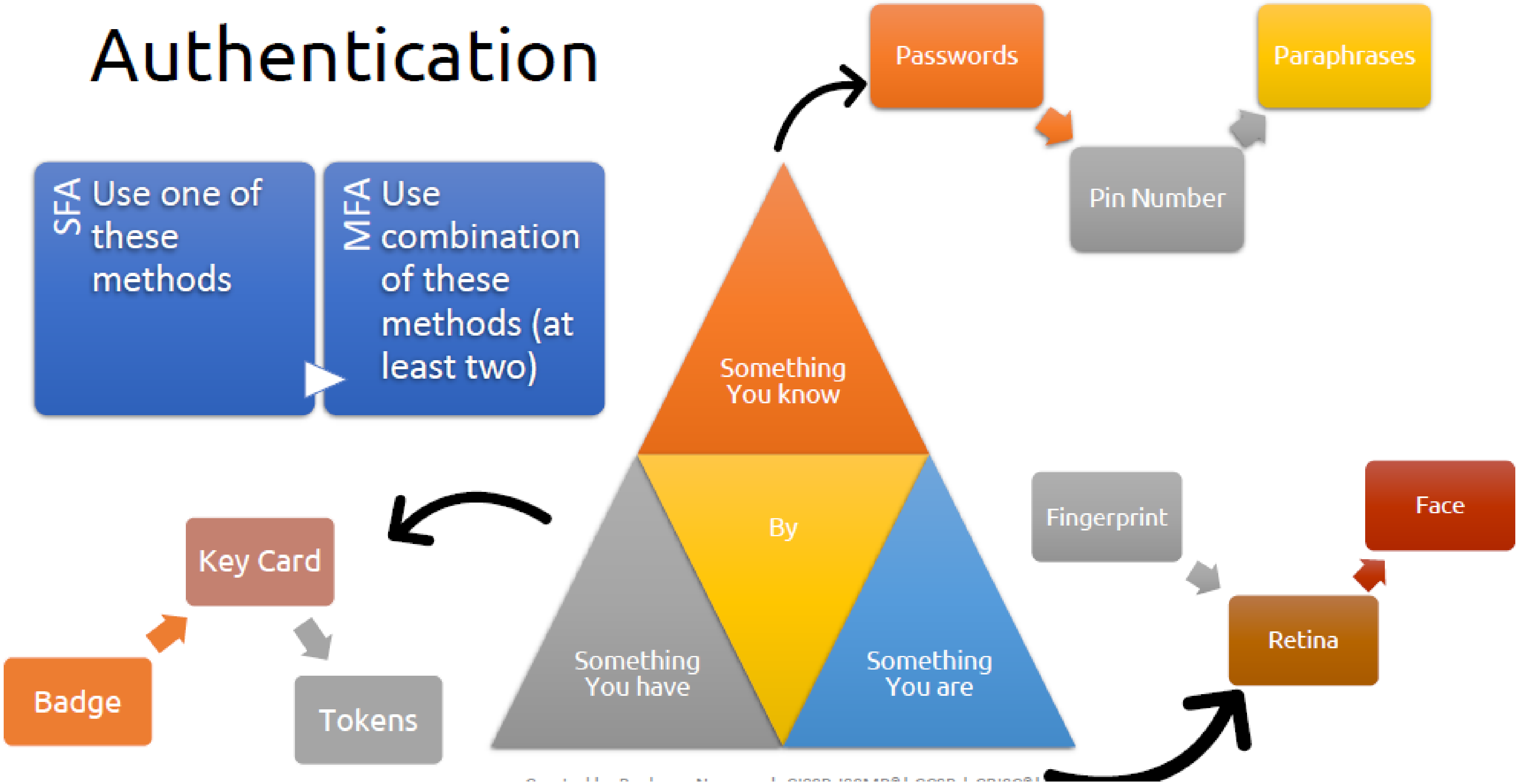
- ❑ Corporate Strategy
  - ✓ Growth
  - ✓ Stability
  - ✓ Renewal
- ❑ Business Strategy
  - ✓ Cost leadership
  - ✓ Differentiation
  - ✓ Market focus
- ❑ Functional Strategy



Strategy Development

- ❑ Desired State
- ❑ Current State
- ❑ Gap Analysis
- ❑ Road Map
- ❑ Resources
- ❑ Constraints

Authentication



SFA: Use one of these methods

MFA: Use combination of these methods (at least two)

Something You know

By

Something You have

Something You are

Passwords

Pin Number

Paraphrases

Key Card

Badge

Tokens

Fingerprint

Retina

Face

Method of Authentications

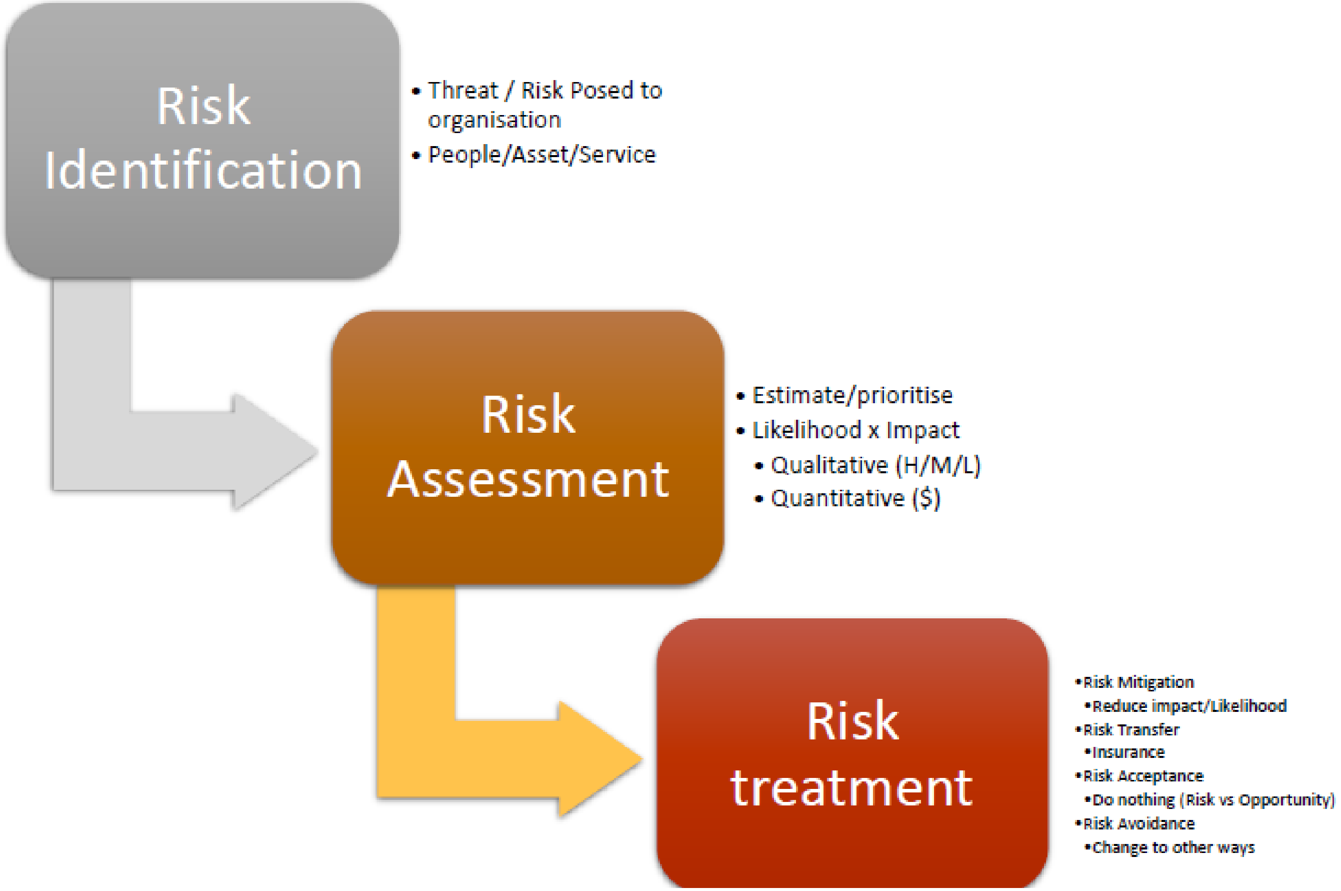
Non-repudiation

- Ensure that the person who does something cannot deny what have done

Privacy

- the right of personnel to control their information

Risk Management



Risk Identification

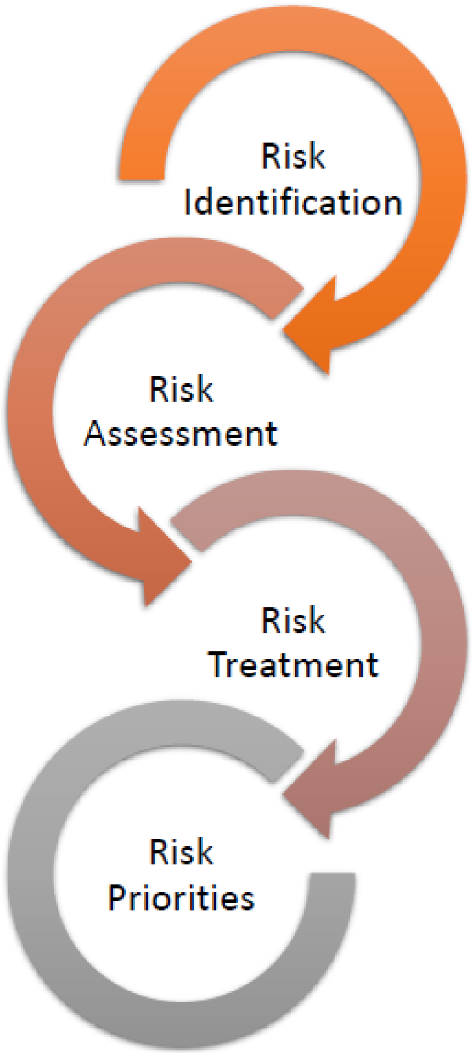
- Threat / Risk Posed to organisation
- People/Asset/Service

Risk Assessment

- Estimate/prioritise
- Likelihood x Impact
  - Qualitative (H/M/L)
  - Quantitative ($)

Risk treatment

- Risk Mitigation
  - Reduce impact/Likelihood
- Risk Transfer
  - Insurance
- Risk Acceptance
  - Do nothing (Risk vs Opportunity)
- Risk Avoidance
  - Change to other ways



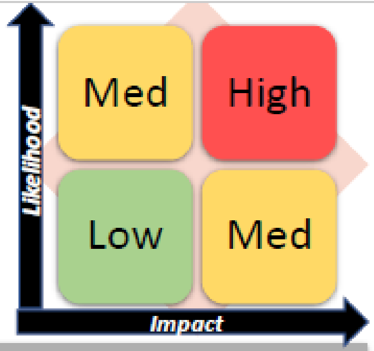
Risk Identification

Risk Assessment

Risk Treatment

Risk Priorities

Risk Priorities / Risk Tolerance



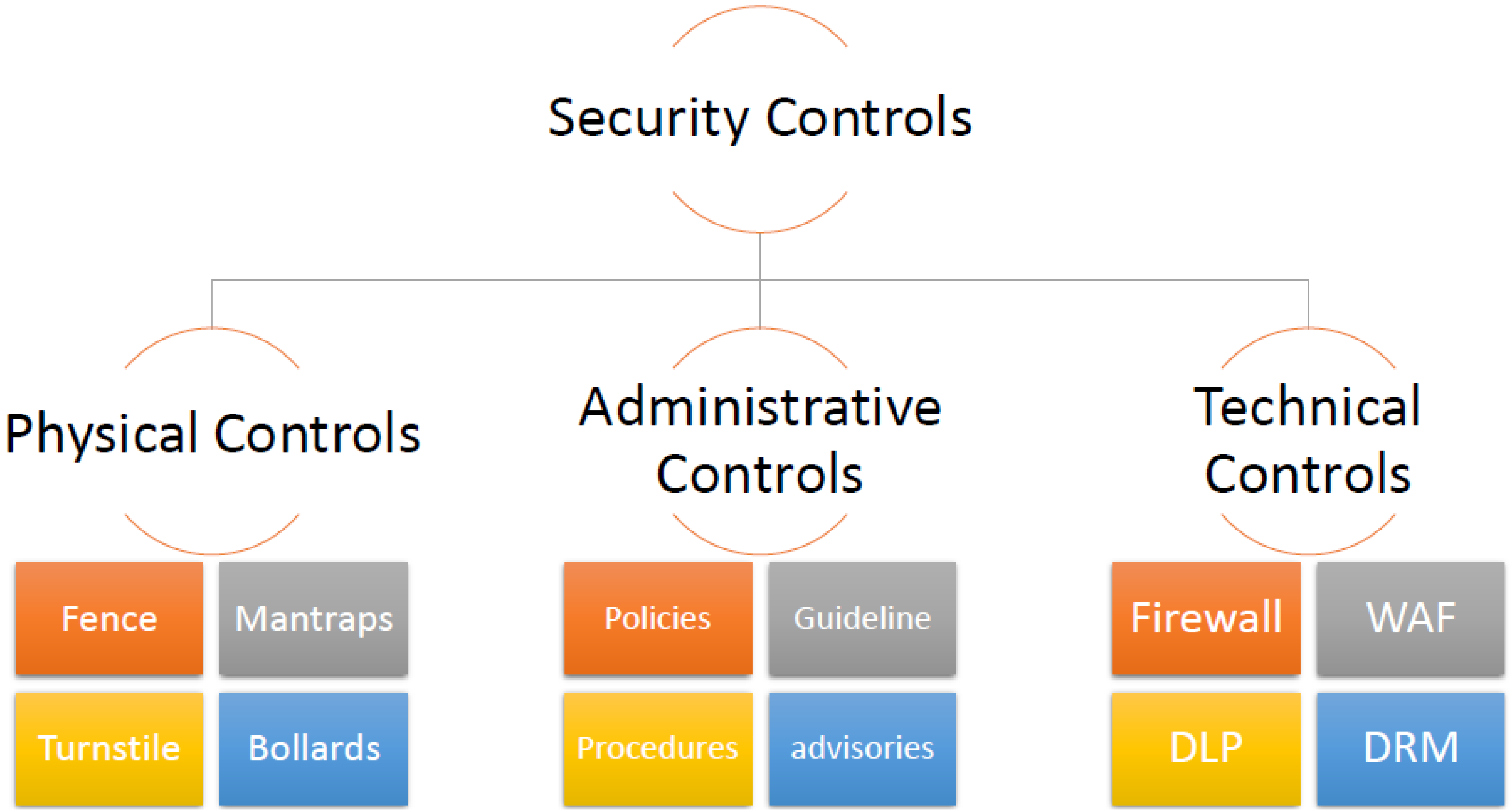
Risk Priorities

- Priority based on Impact x Likelihood
- Help in prioritising risk treatment

Risk Tolerance

- Limit of level of risk, acceptable by senior management (associated with risk appetite)

Security Controls



Governance

Regulations/Laws

- HIPPA (Medical records)
- GDPR (PII)

Policies (Broad)

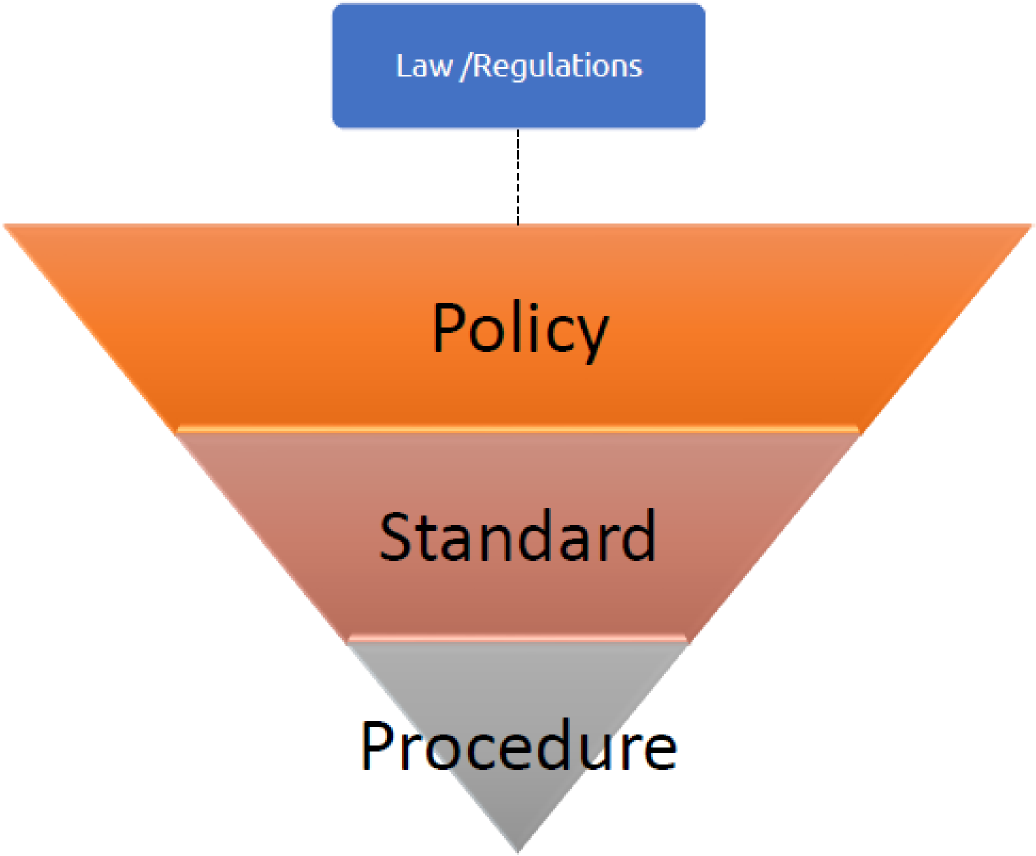
- AUP
- Access Control Policy

Standard (may include technical controls)

- ISO
- NIST
- PCI DSS

Procedures (Day-to-Day Operations)

- Special Tasks
- routine activities



Law /Regulations

Policy

Standard

Procedure

Code of Ethics

Preamble

- The safety and welfare of society and the common good, duty to our principals, and to each other
- Certified holders must adherence to this Code is a condition of certification

Canons

- Protect society, the common good, necessary public trust and confidence, and the infrastructure
- Act honorably, honestly, justly, responsibly and legally
- Provide diligent and competent service to principals
- Advance and protect the profession

Chapter 2 : IR/BC/DR

Breach
Incident
Intrusion
Event
Vulnerability
Exploit
Threat
Zero-Day

Goal of IR

- To reduce impact of incident

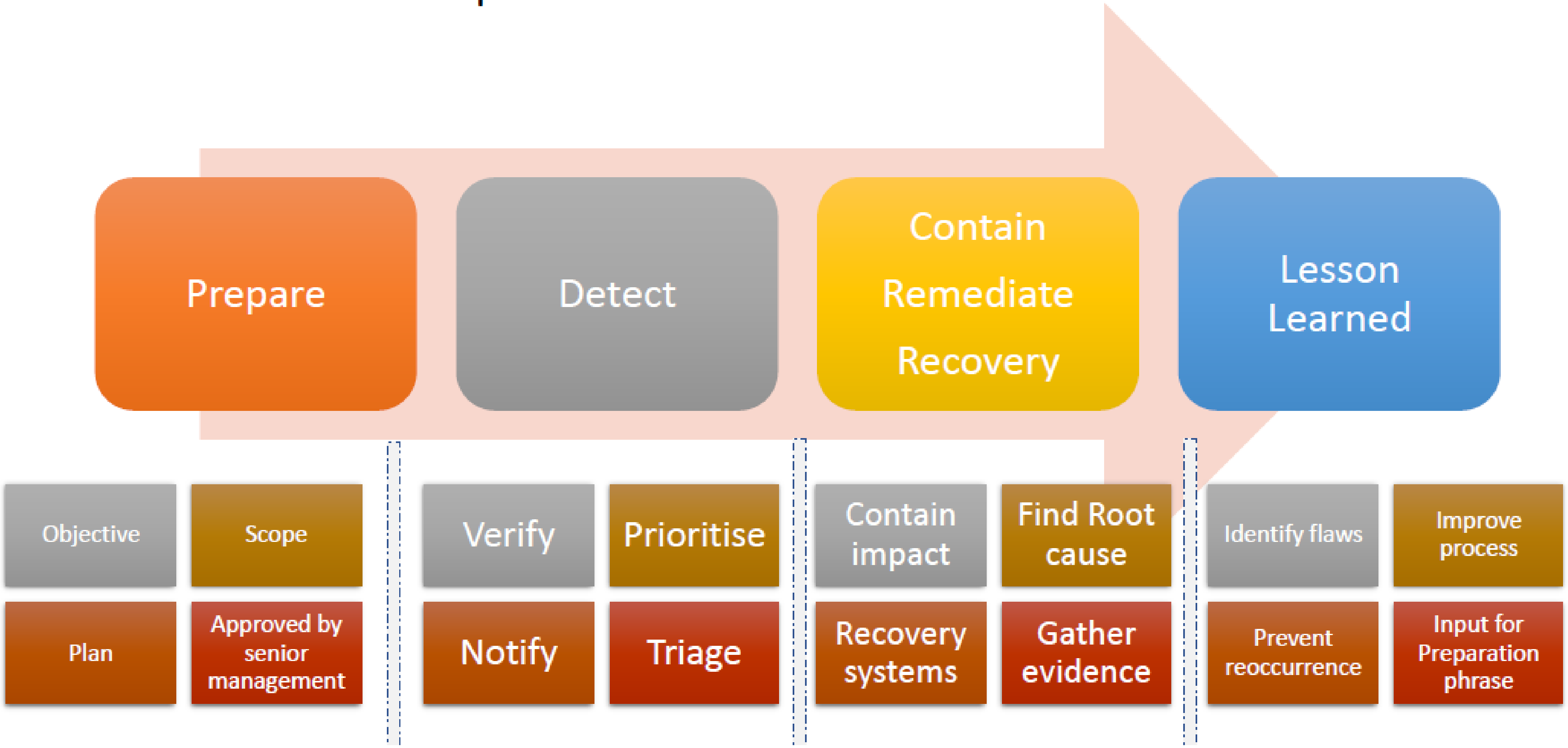
Goal of BC

- To keep critical operation running during the right of personnel to control their information disaster

DR

- To get operation back to normal state during disaster

Incident Response Processes



Prepare

Detect

Contain
Remediate
Recovery

Lesson Learned

Objective

Scope

Plan

Approved by senior management

Verify

Prioritise

Notify

Triage

Contain impact

Find Root cause

Recovery systems

Gather evidence

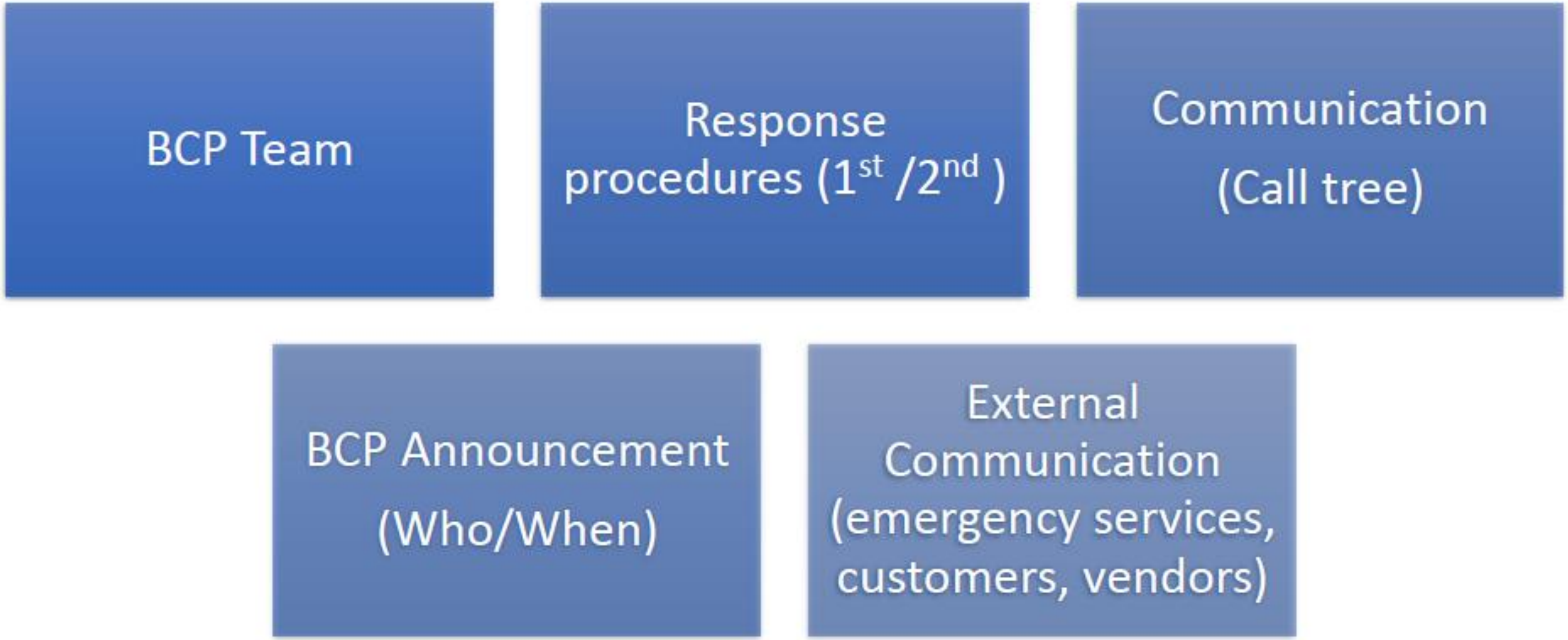
Identify flaws

Improve process

Prevent reoccurrence

Input for Preparation phrase

Business Continuity



BCP Team

Response procedures (1st /2nd)

Communication

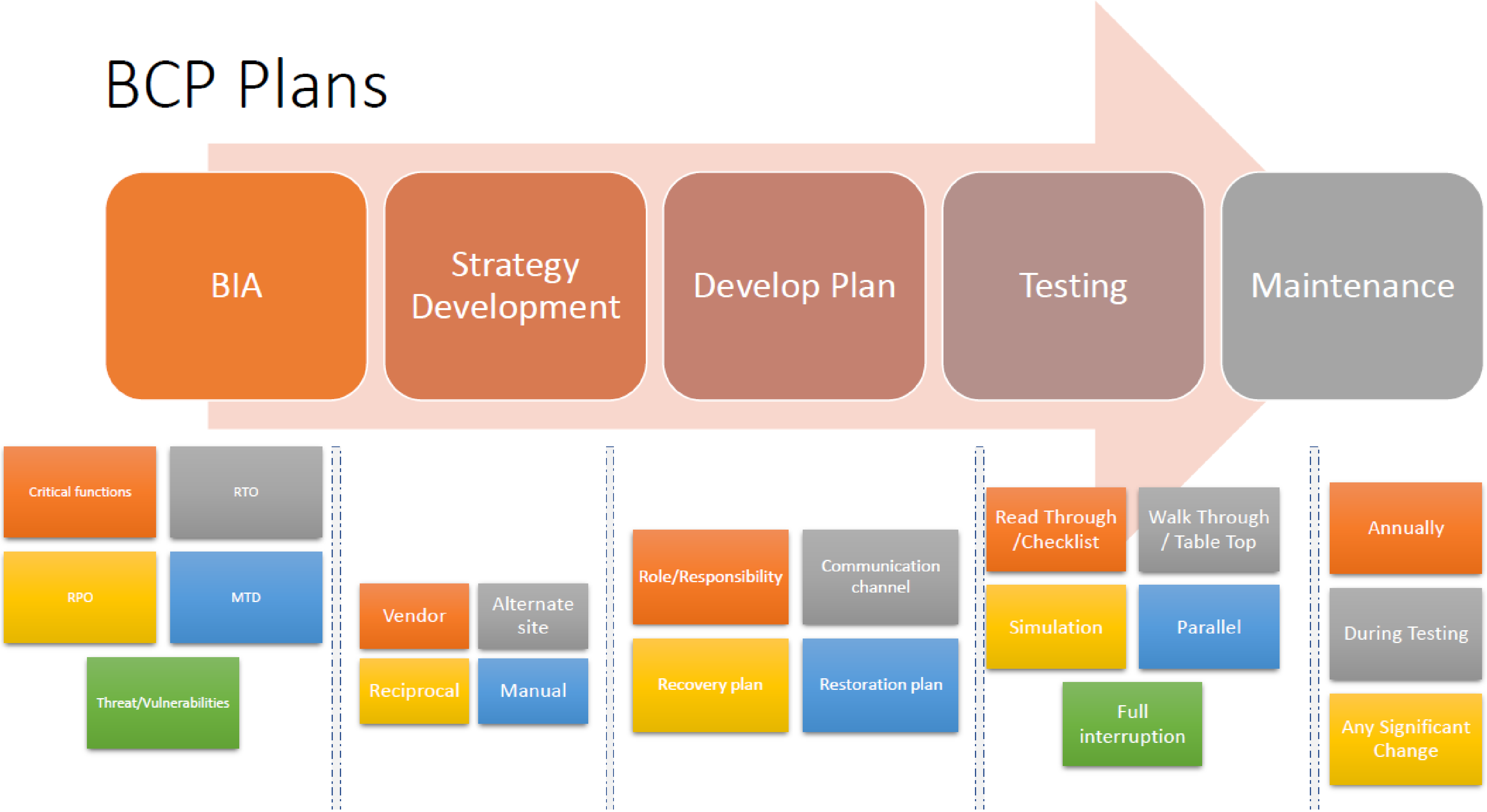
(Call tree)

BCP Announcement

(Who/When)

External Communication (emergency services, customers, vendors)

BCP Plans



BIA
- Critical functions
- RTO
- RPO
- MTD
- Threat/Vulnerabilities

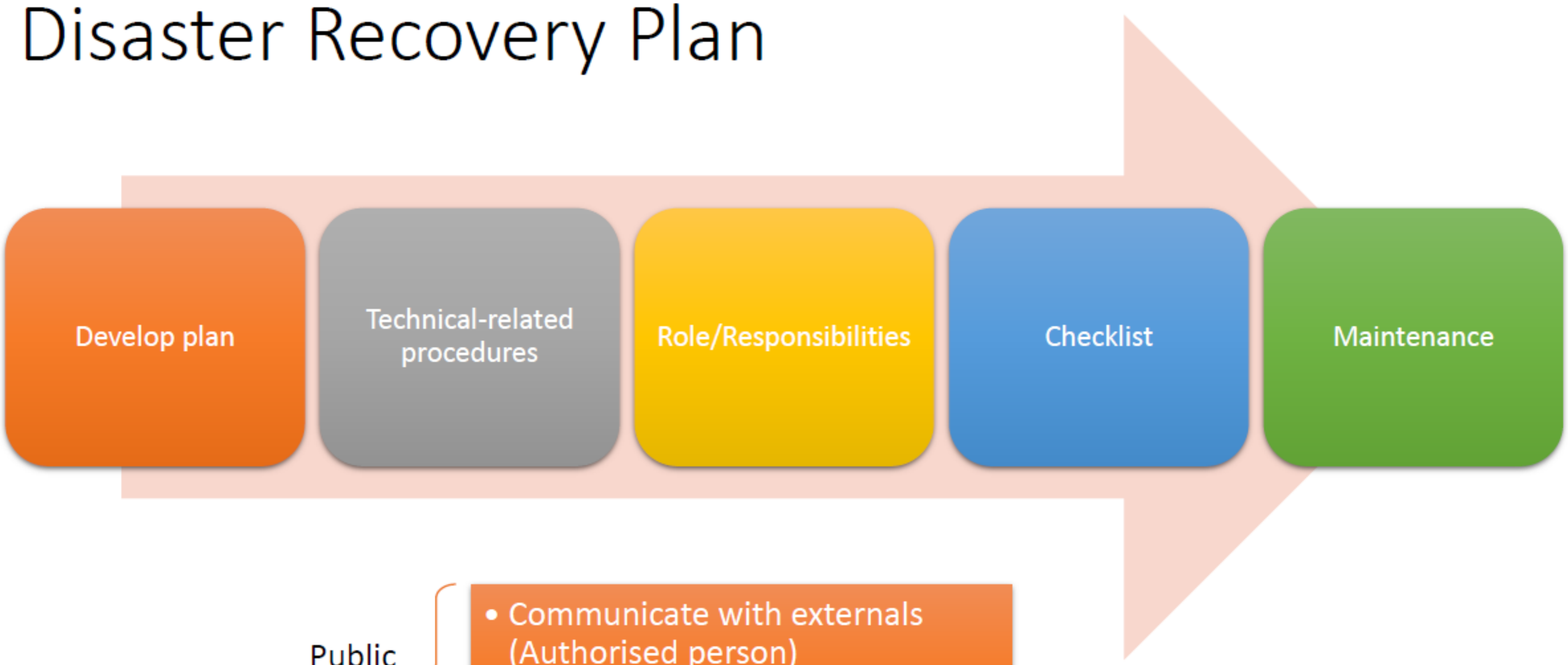
Strategy Development
- Vendor
- Alternate site
- Reciprocal
- Manual

Develop Plan
- Role/Responsibility
- Communication channel
- Recovery plan
- Restoration plan

Testing
- Read Through /Checklist
- Walk Through / Table Top
- Simulation
- Parallel
- Full interruption

Maintenance
- Annually
- During Testing
- Any Significant Change

Disaster Recovery Plan



Develop plan

Technical-related procedures

Role/Responsibilities

Checklist

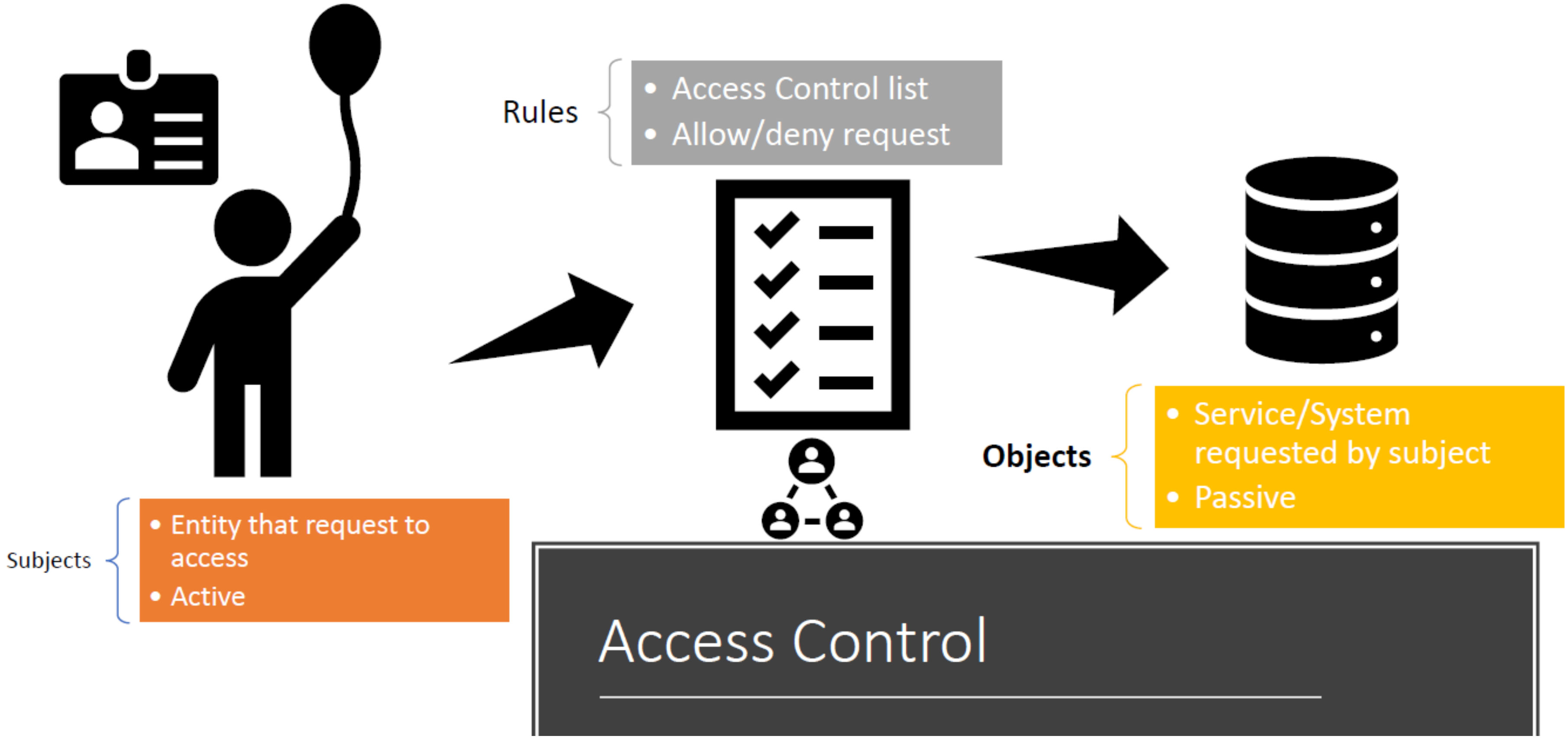
Maintenance

Public relation

- Communicate with externals (Authorised person)
- Contents will be decided by management

Checklist

- Will help prioritising step and procedures during crisis occurred



Rules

- Access Control list
- Allow/deny request

Objects

- Service/System requested by subject
- Passive

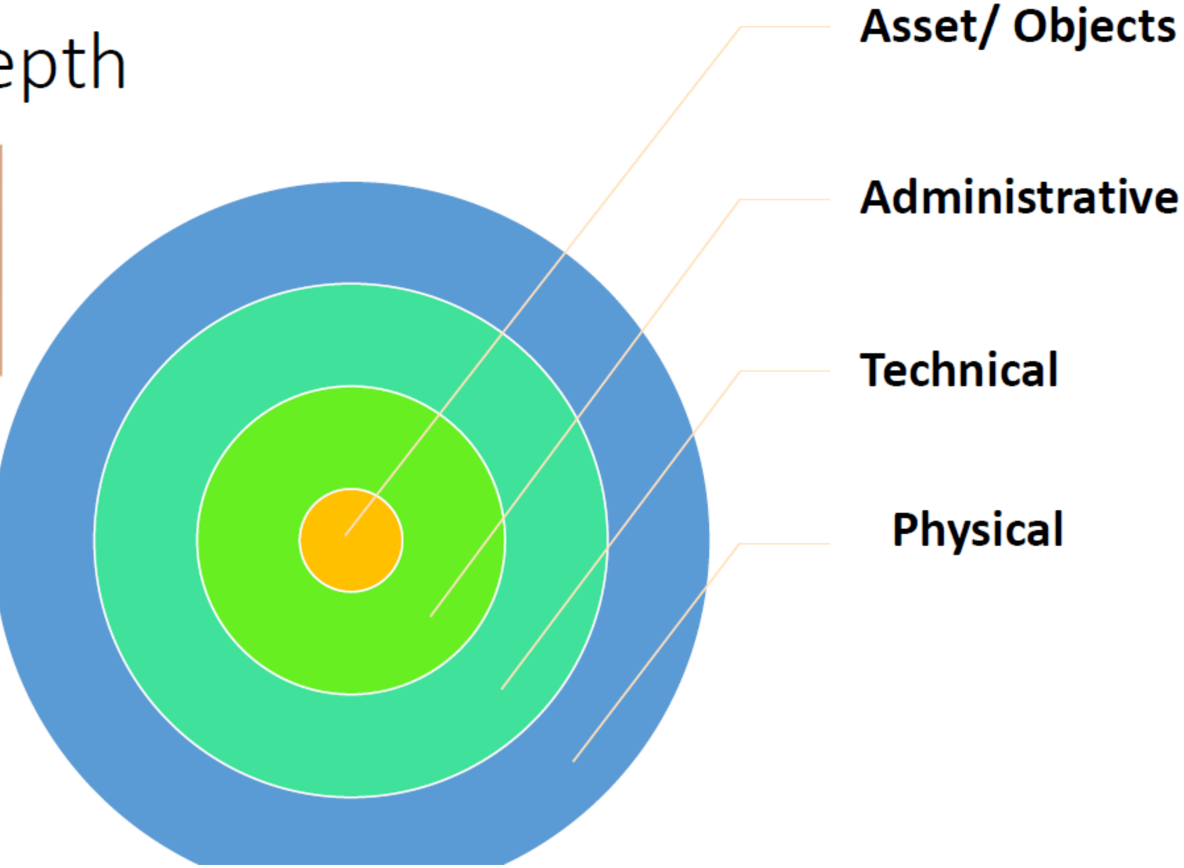
Subjects

- Entity that request to access
- Active

Access Control

Defence in Depth

Multiple layers of controls for increasing security



Asset/ Objects

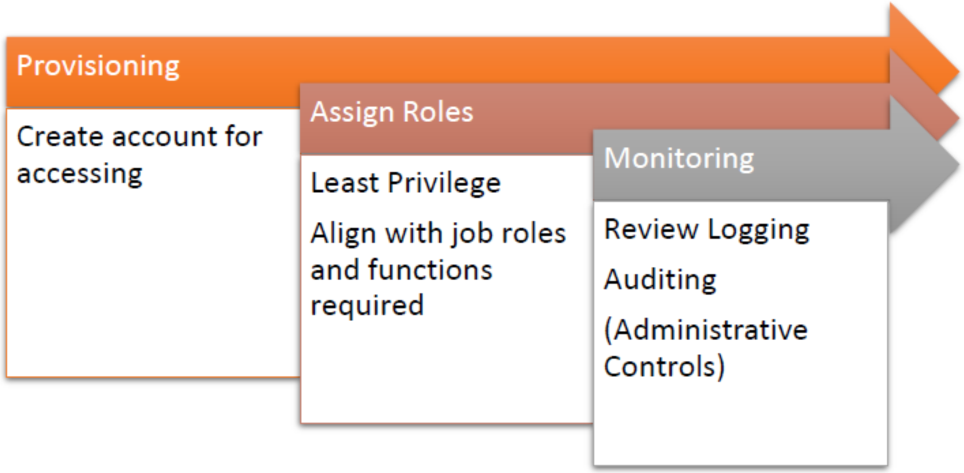
Administrative

Technical

Physical

Control Assessment – to measure the effectiveness of control (as intended)

Privileged Access Management



Provisioning

Create account for accessing

Assign Roles

Least Privilege

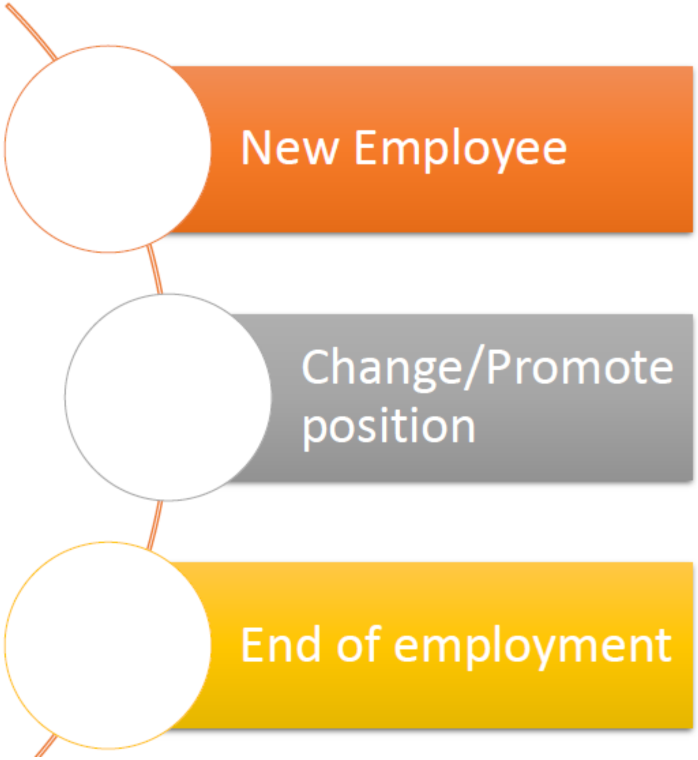
Align with job roles and functions required

Monitoring

Review Logging

Auditing

(Administrative Controls)



New Employee

Change/Promote position

End of employment

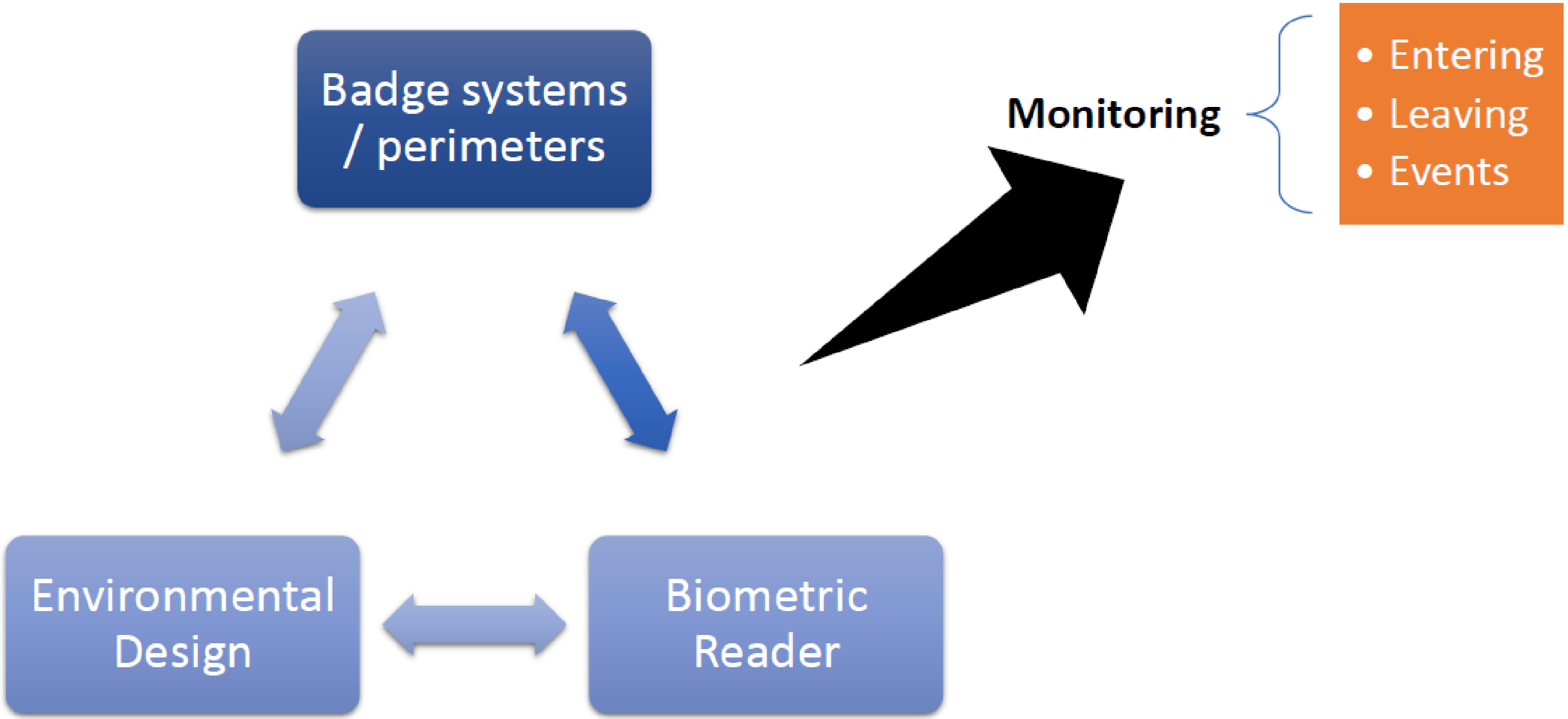
Segregation of Duties

- Separate related tasks and responsibilities

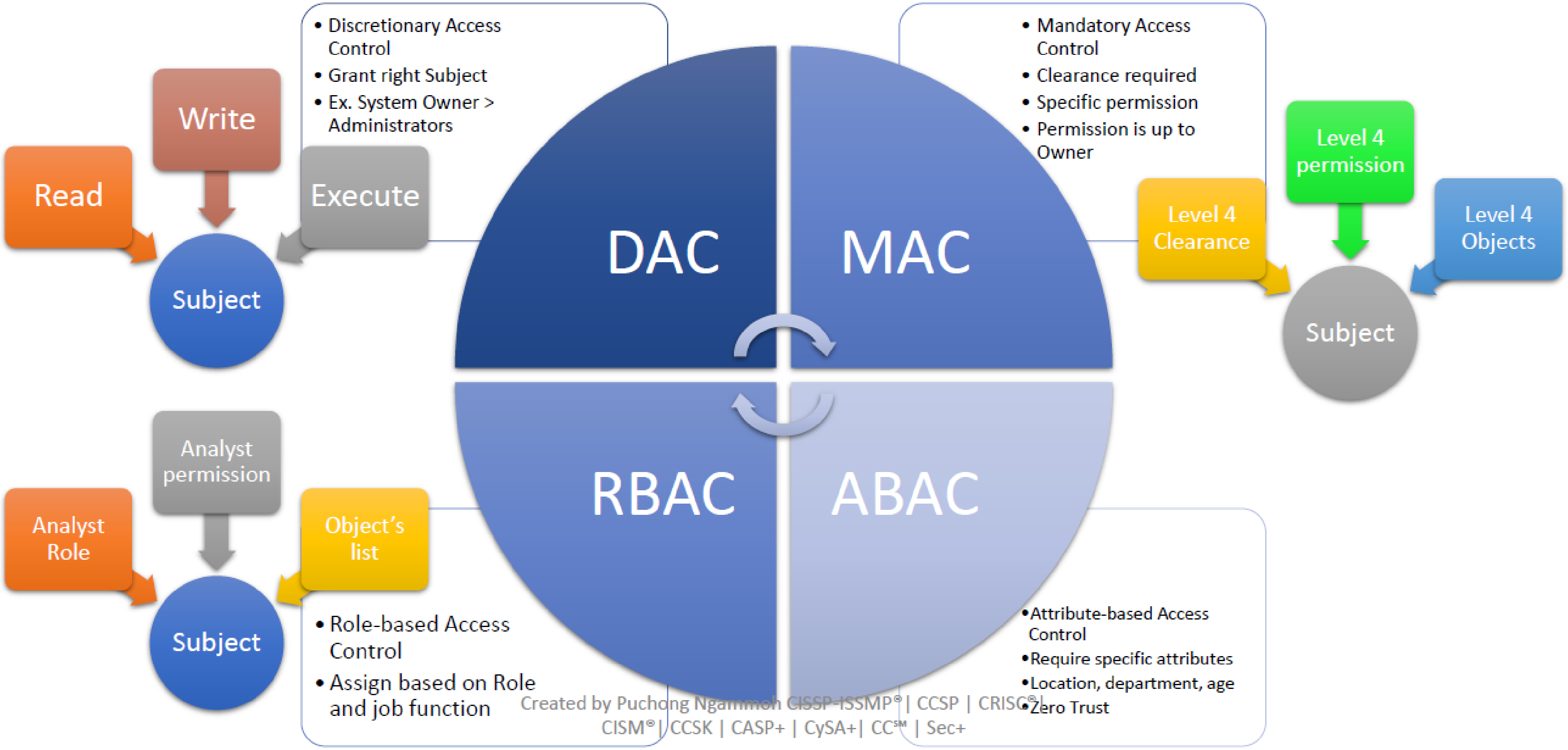
Two-person

- Prevent Frauds and insider threat
- High security task/area

Access Control methods



Access Control methods



- Discretionary Access Control
- Grant right Subject
- Ex. System Owner > Administrators

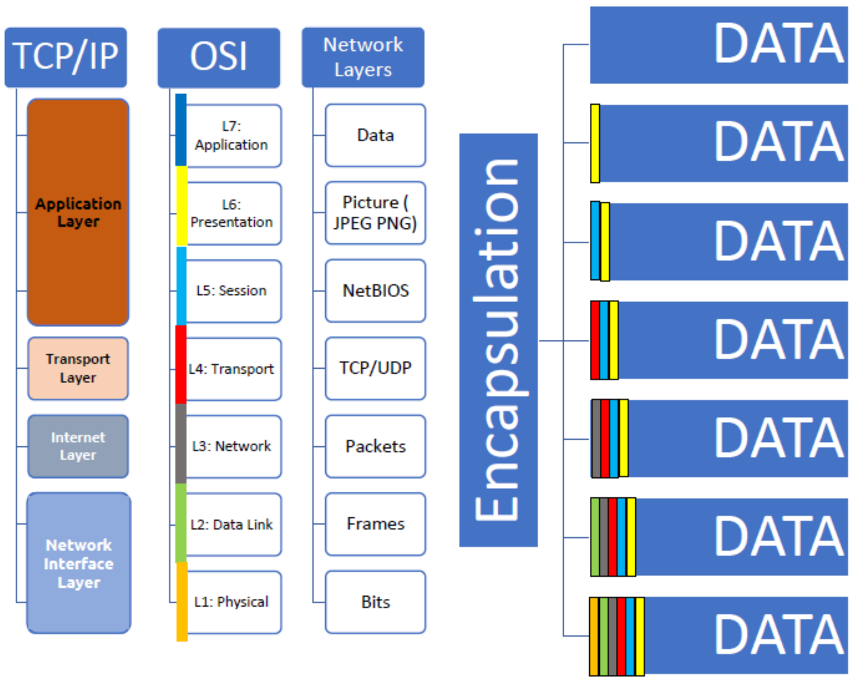
- Mandatory Access Control
- Clearance required
- Specific permission
- Permission is up to Owner

- Role-based Access Control
- Assign based on Role and job function

- Attribute-based Access Control
- Require specific attributes
- Location, department, age
- Zero Trust

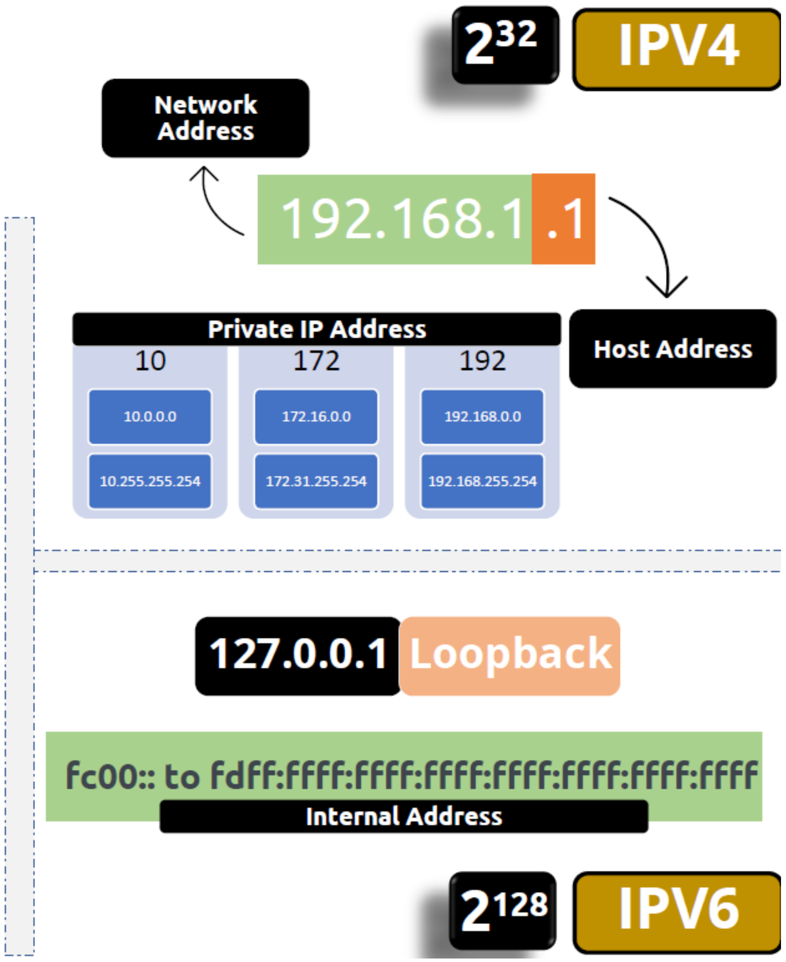
Created by Puchong Ngammoh CISSP-ISSMP® | CCSP | CRISC® | CISM® | CCSK | CASP+ | CySA+| CC℠ | Sec+

Domain 4 : Networking



TCP/IP	OSI	Network Layers
Application Layer	L7: Application	Data
	L6: Presentation	Picture (JPEG PNG)
	L5: Session	NetBIOS
Transport Layer	L4: Transport	TCP/UDP
Internet Layer	L3: Network	Packets
Network Interface Layer	L2: Data Link	Frames
	L1: Physical	Bits

Created by Puchong Ngammoh CISSP-ISSMP® | CCSP | CRISC® | CISM® | CCSK | CASP+ | CySA+| CC℠ | Sec+



Private IP Address

10	172	192
10.0.0.0	172.16.0.0	192.168.0.0
10.255.255.254	172.31.255.254	192.168.255.254

Port/Protocols

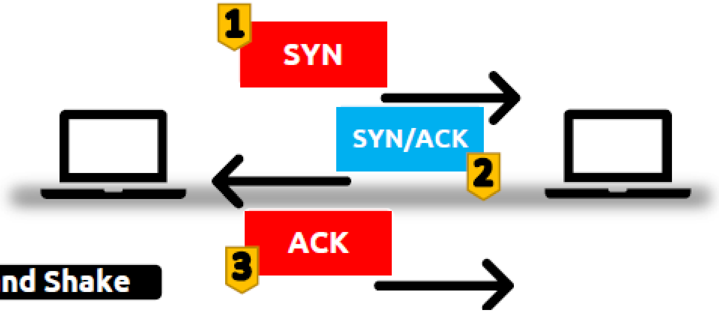
Physical Ports

CAT5E	Fiber optic	CAT6
1 (Mbit/s)	1	1
100 MHz	10 Gbps	250 MHz

Logical Ports

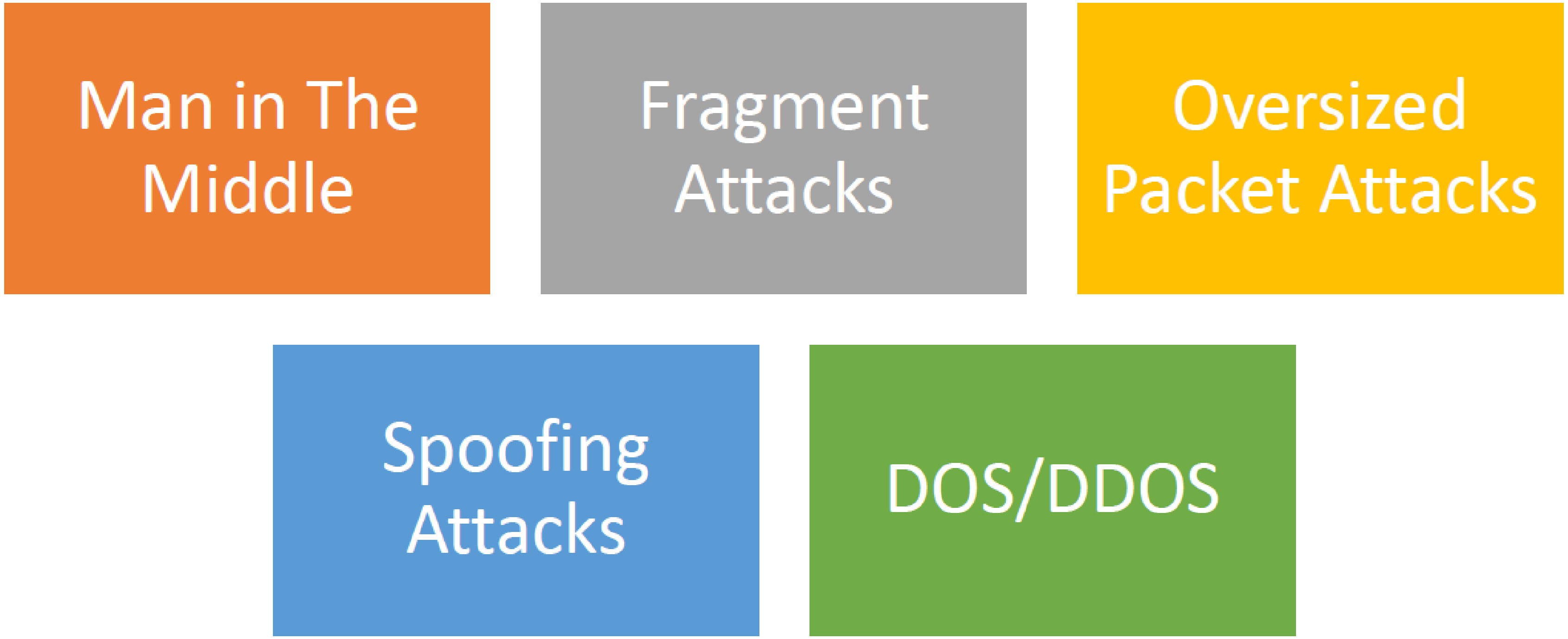
Well-known	Registered	Dynamic/Private
0	1024	49152
1023	49151	65535

21	FTP	22	SFTP
23	Telnet	22	SSH
25	SMTP	587	SMTP
37	Time	123	NTP
53	DNS	853	DoT
80	HTTP	443	HTTPS
161	SNMP	161	SNMP
445	SMB	2049	NFS
389	LDAP	636	LDAPS



3 ways Hand Shake

Wireless Network Threat



Man in The Middle

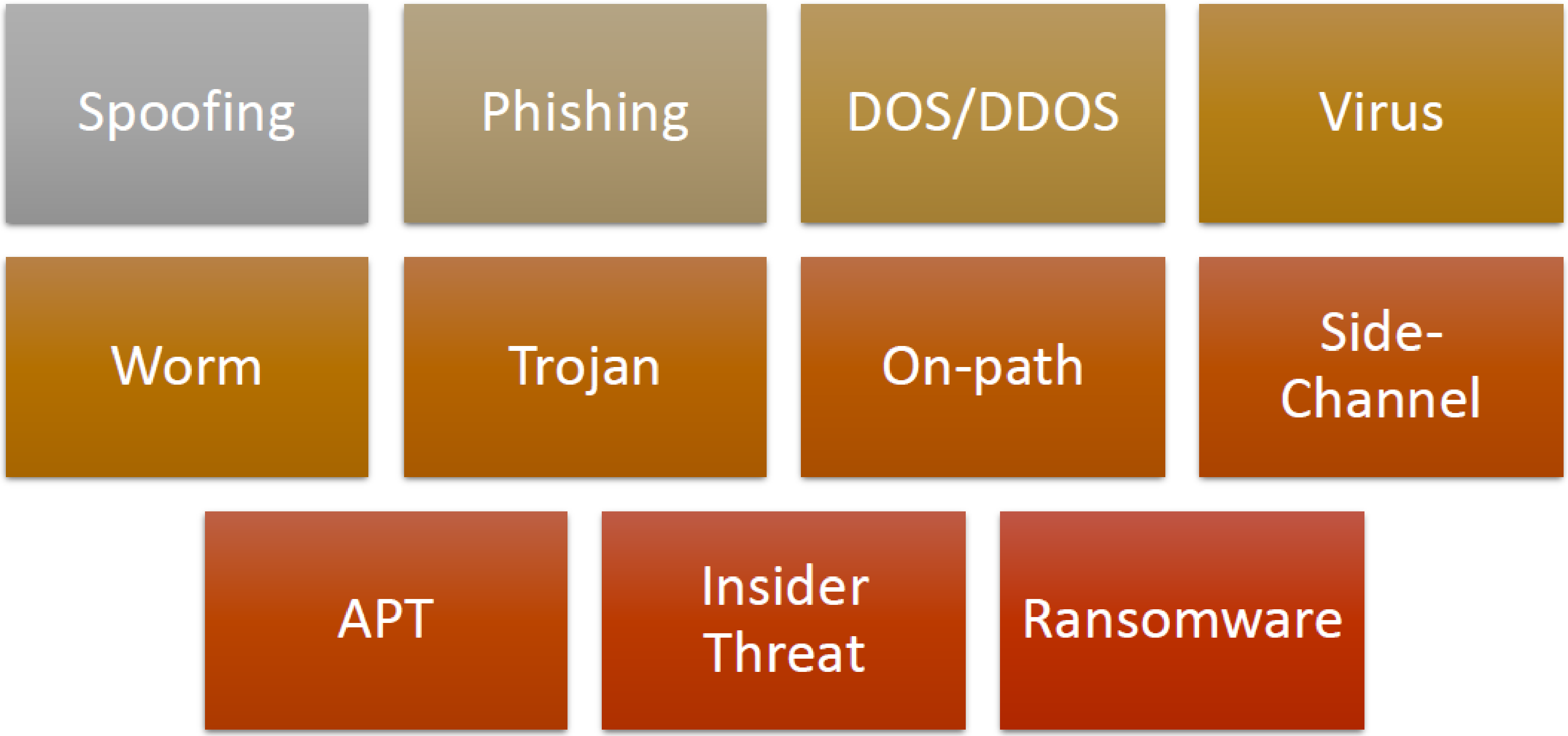
Fragment Attacks

Oversized Packet Attacks

Spoofing Attacks

DOS/DDOS

Cyber Threat



Spoofing

Phishing

DOS/DDOS

Virus

Worm

Trojan

On-path

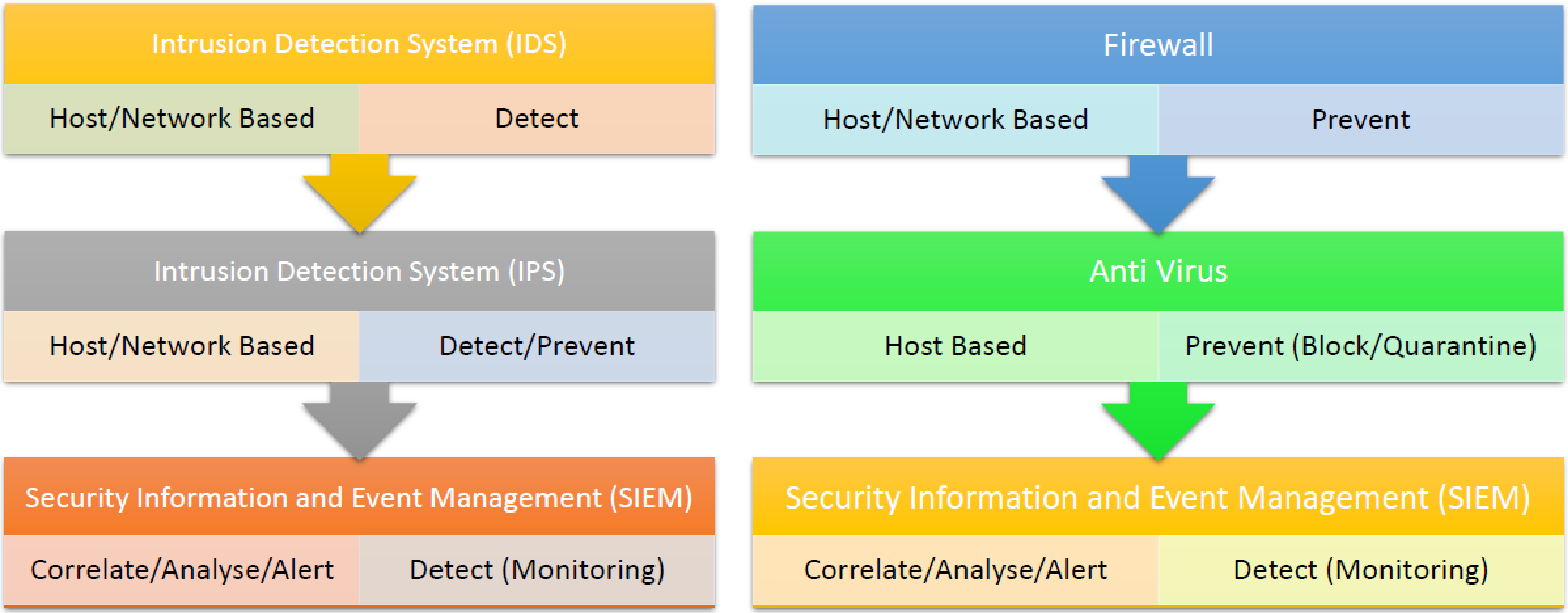
Side-Channel

APT

Insider Threat

Ransomware

Preventing/Detecting Threats



Intrusion Detection System (IDS)

Host/Network Based | Detect

Intrusion Detection System (IPS)

Host/Network Based | Detect/Prevent

Security Information and Event Management (SIEM)

Correlate/Analyse/Alert | Detect (Monitoring)

Firewall

Host/Network Based | Prevent

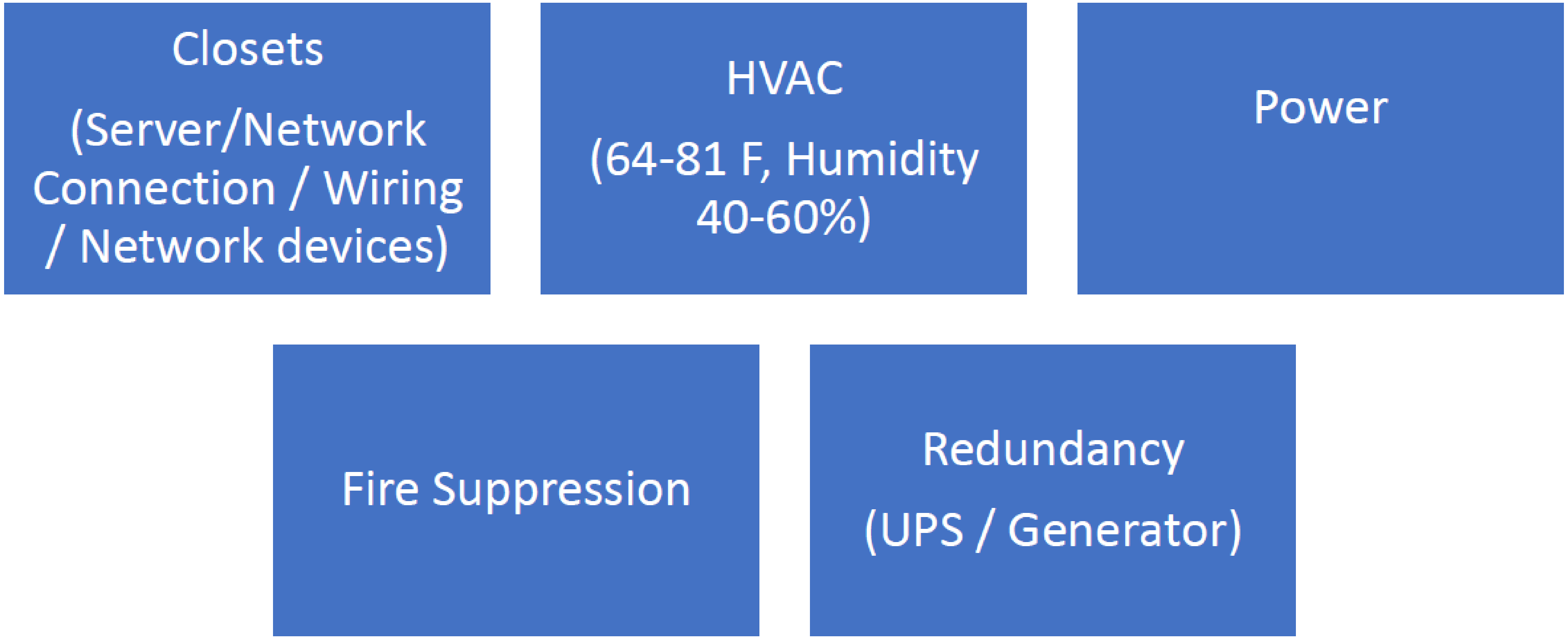
Anti Virus

Host Based | Prevent (Block/Quarantine)

Security Information and Event Management (SIEM)

Correlate/Analyse/Alert | Detect (Monitoring)

Data Centre Components



Closets

(Server/Network Connection / Wiring / Network devices)

HVAC

(64-81 F, Humidity 40-60%)

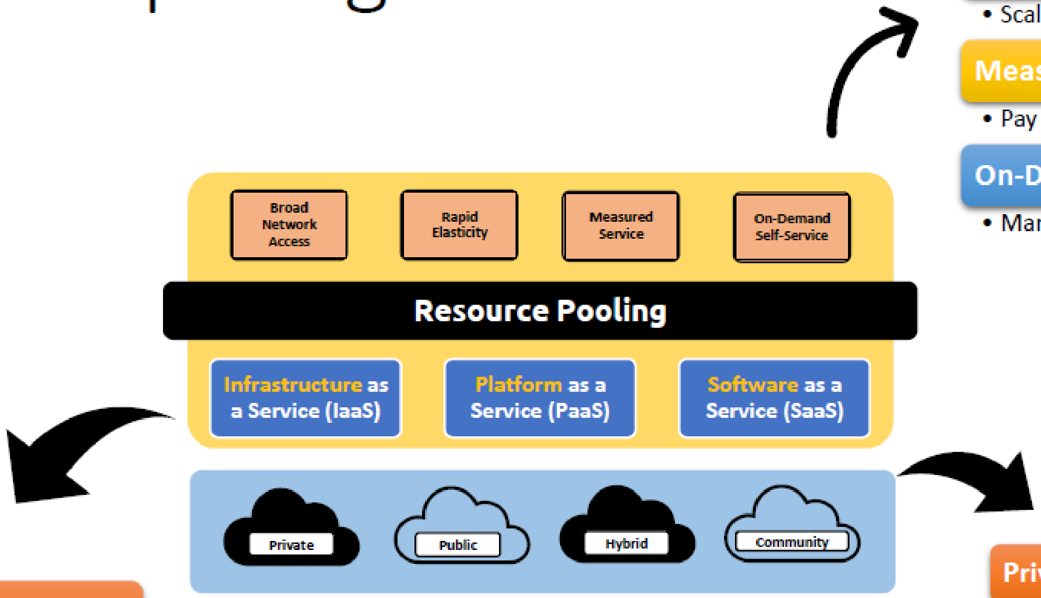
Power

Fire Suppression

Redundancy

(UPS / Generator)

Cloud Computing



Broad Network Access

- Access from anywhere with internet connection

Rapid Elasticity

- Scale up/down based on demands

Measured Service

- Pay as you go

On-Demand Self-Service

- Manage without contacting vendors

Infrastructure as a Service (IaaS)

- CSC Manage the most of components

Platform as a Service (PaaS)

- CSP provide Underlying OS components

Software as a Service (SaaS)

- CSP manage most of the components

Private Cloud

- Solely own by one organisation using own resources

Public Cloud

- Shared resources with other tenants

Hybrid Cloud

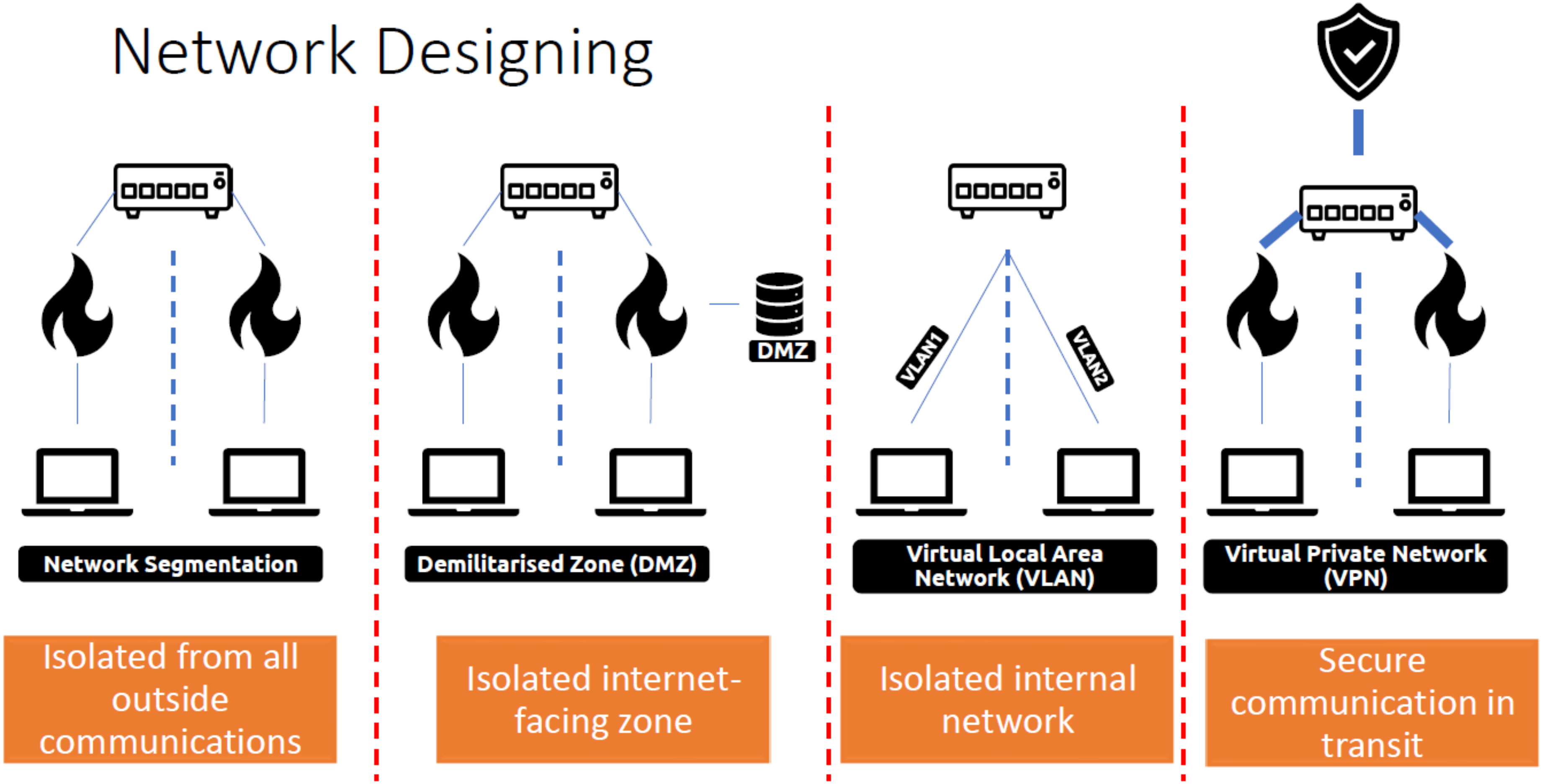
- Combination of one or more cloud deployments

Community Cloud

- Affinity Group on same objectives

Created by Puchong Ngammoh CISSP-ISSMP® | CCSP | CRISC® |

Network Designing



Network Segmentation

Isolated from all outside communications

Demilitarised Zone (DMZ)

Isolated internet-facing zone

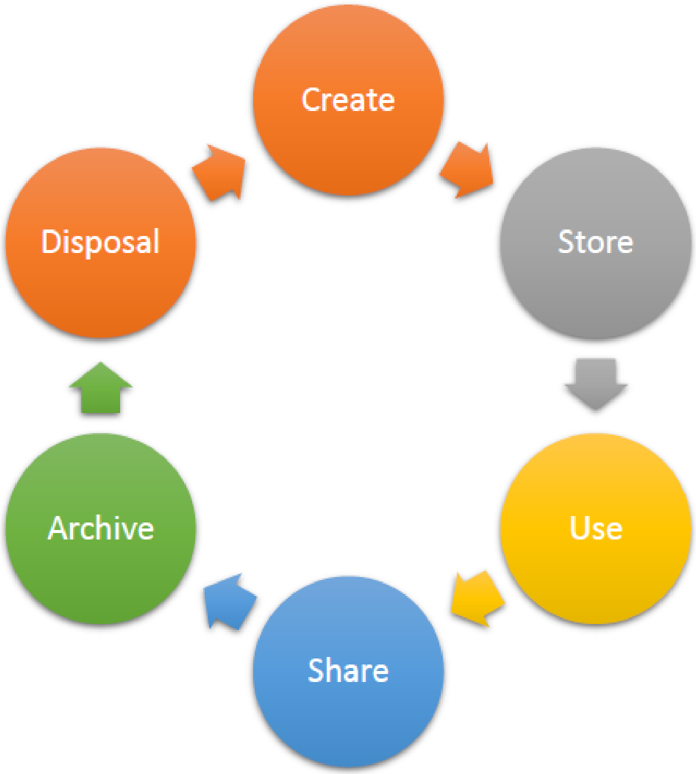
Virtual Local Area Network (VLAN)

Isolated internal network

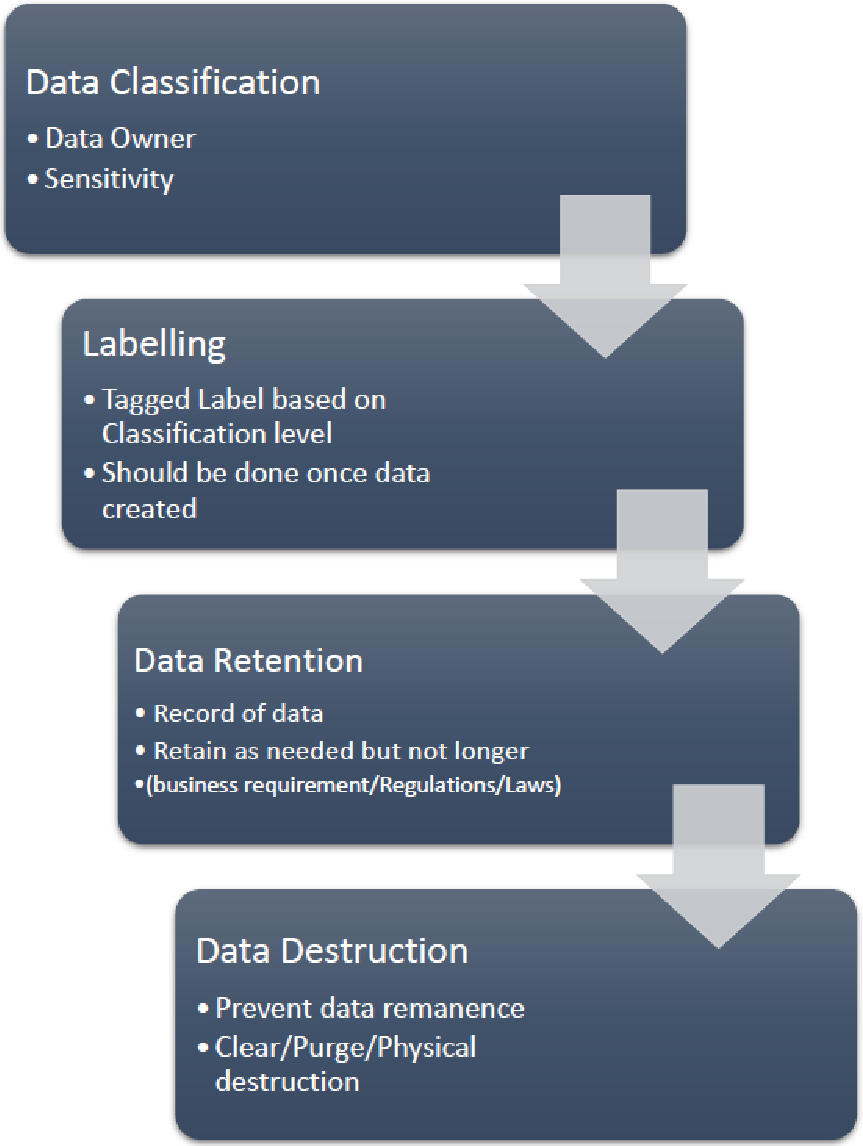
Virtual Private Network (VPN)

Secure communication in transit

Data Life cycle



Created by Puchong Ngammoh CISSP-ISSMP® | CCSP | CRISC® | CISM® | CCSK | CASP+ | CySA+ | CC℠ | Sec+



Data Classification

- Data Owner
- Sensitivity

Labelling

- Tagged Label based on Classification level
- Should be done once data created

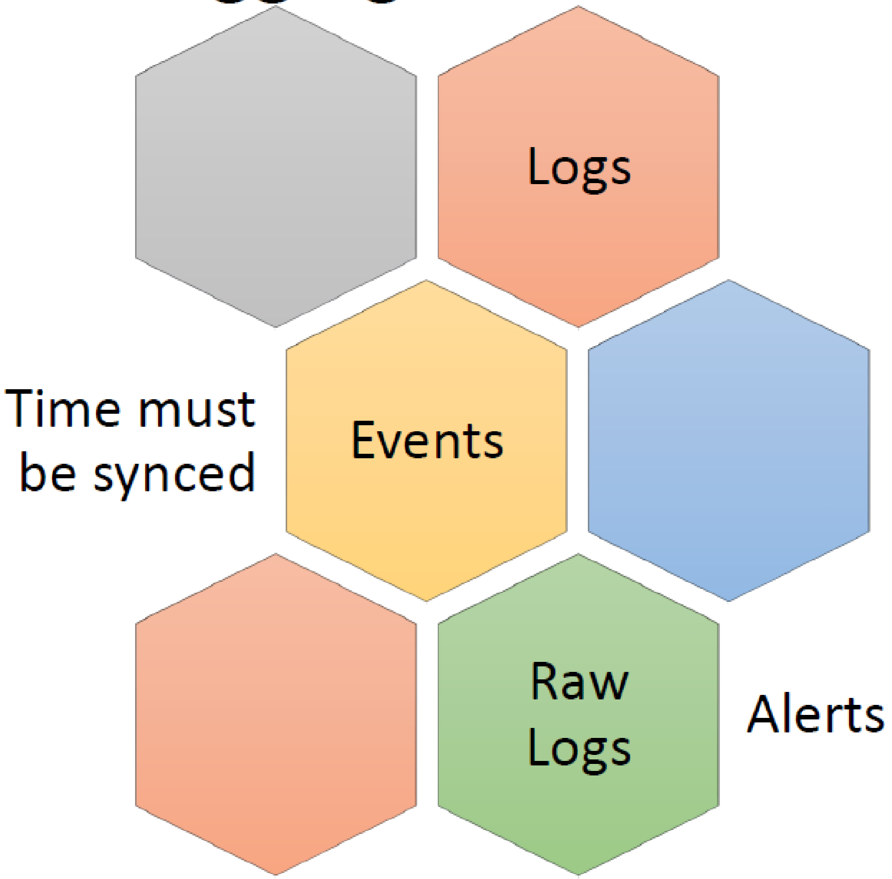
Data Retention

- Record of data
- Retain as needed but not longer
- (business requirement/Regulations/Laws)

Data Destruction

- Prevent data remanence
- Clear/Purge/Physical destruction

Logging and Monitoring



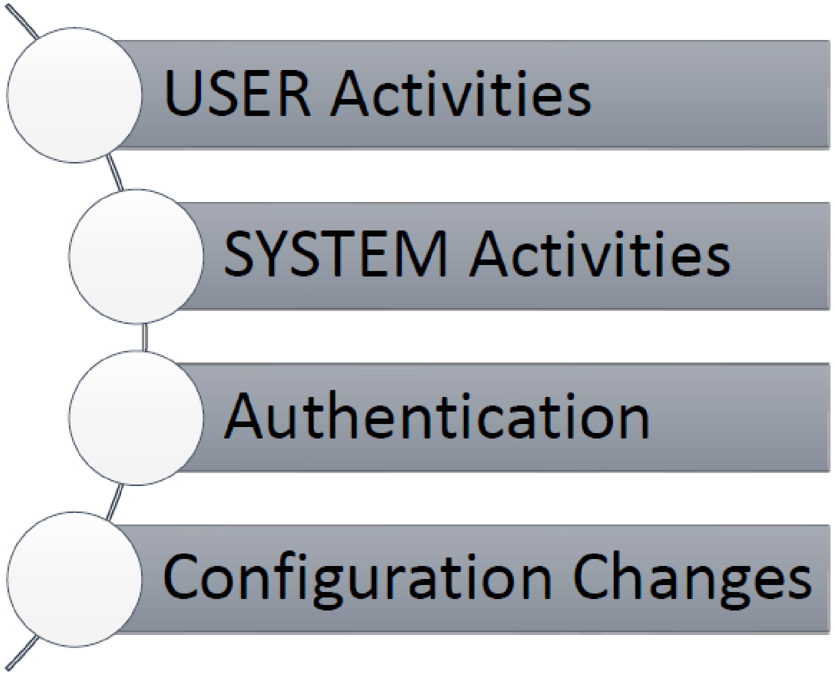
Logs

Time must be synced

Events

Raw Logs

Alerts



USER Activities

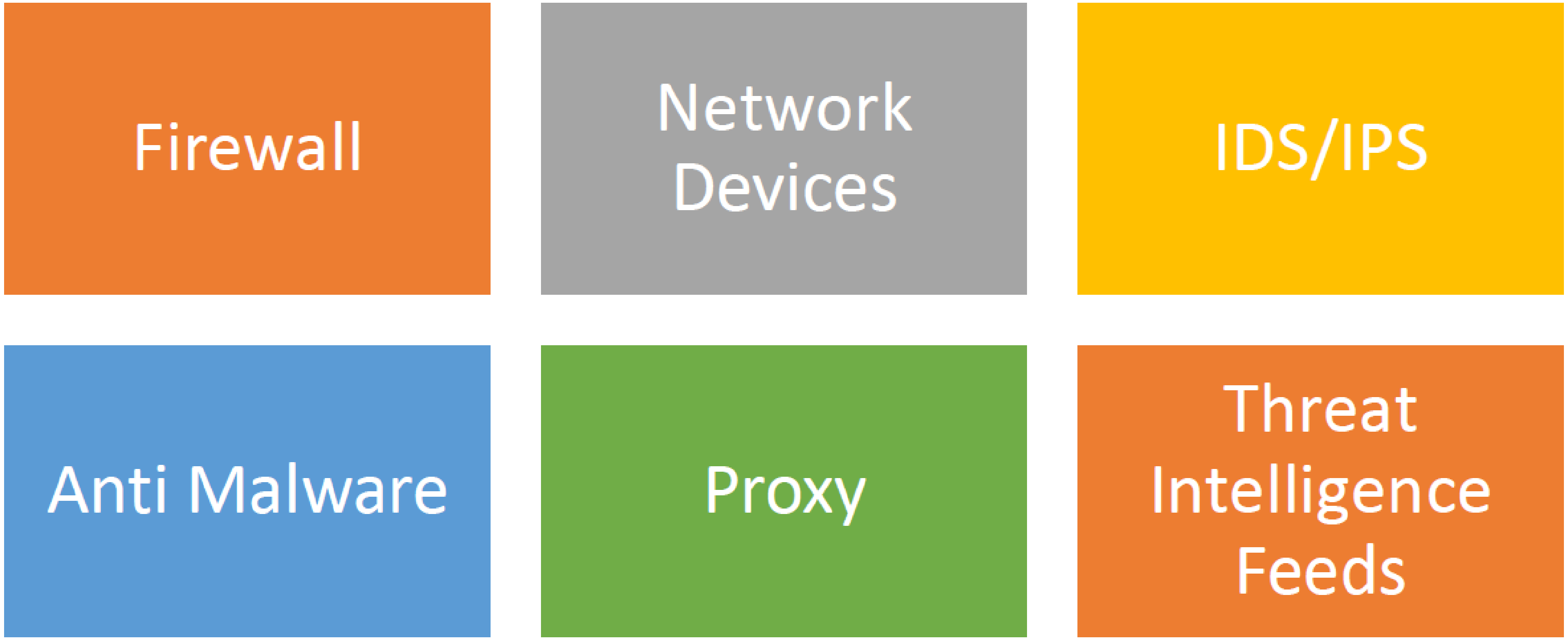
SYSTEM Activities

Authentication

Configuration Changes

Created by Puchong Ngammoh CISSP-ISSMP®| CCSP | CR
CISM®| CCSK | CASP+ | CySA+| CC℠ | Sec+

Common Log Sources



Firewall

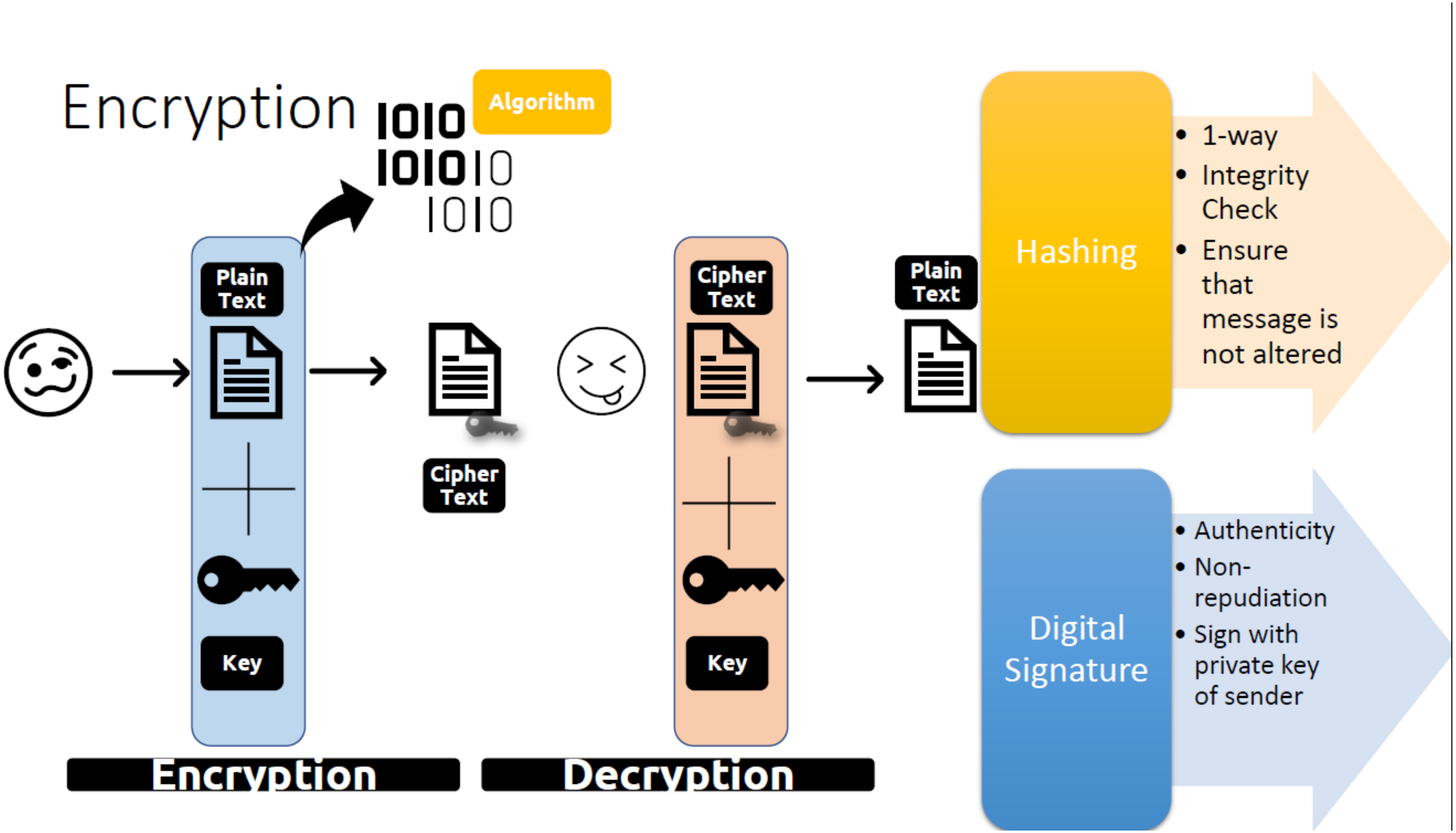
Network Devices

IDS/IPS

Anti Malware

Proxy

Threat Intelligence Feeds



Encryption

1010
101010
1010

Algorithm

Plain Text

Key

Cipher Text

Cipher Text

Key

Plain Text

Encryption

Decryption

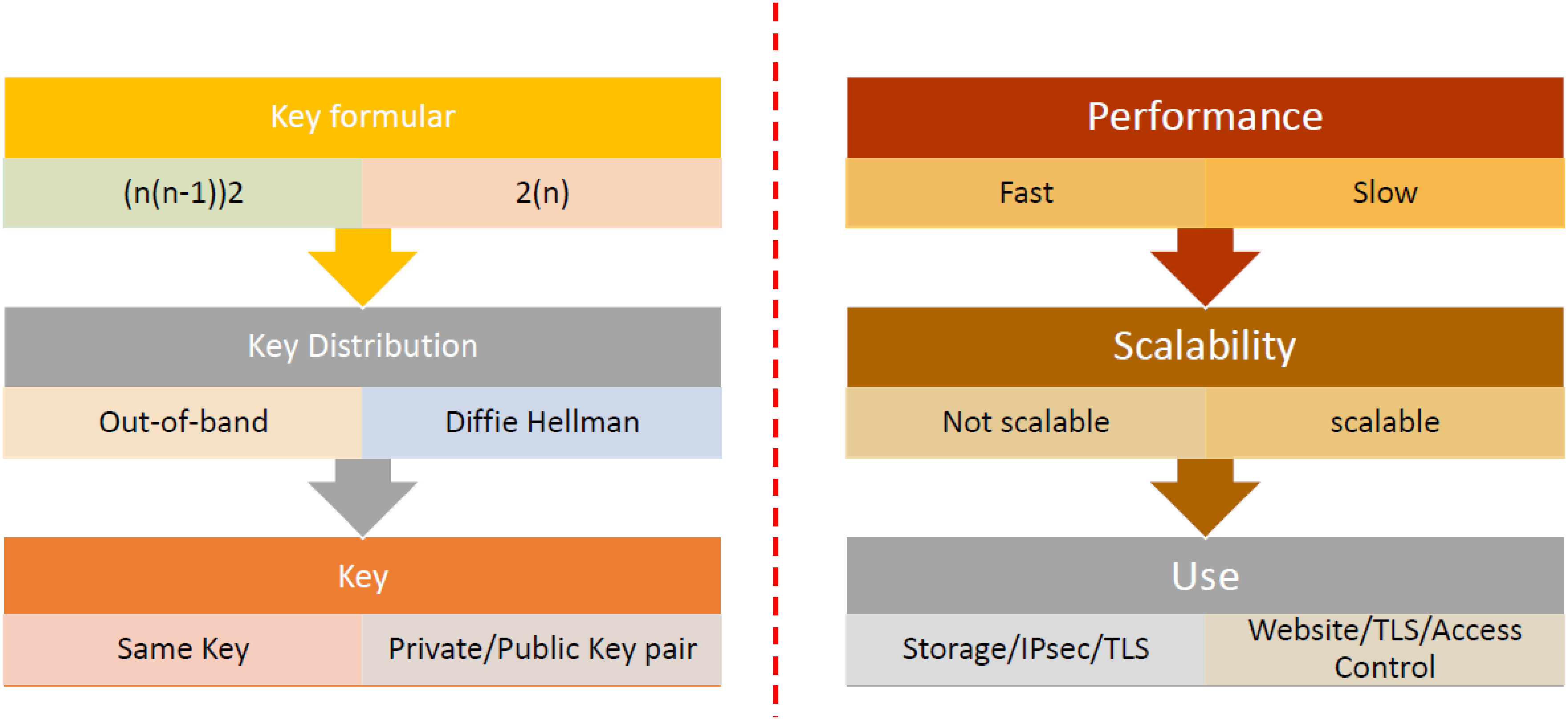
Hashing

- 1-way
- Integrity Check
- Ensure that message is not altered

Digital Signature

- Authenticity
- Non-repudiation
- Sign with private key of sender

Symmetric / Asymmetric



Key formular

(n(n-1))2 | 2(n)

Key Distribution

Out-of-band | Diffie Hellman

Key

Same Key | Private/Public Key pair

Performance

Fast | Slow

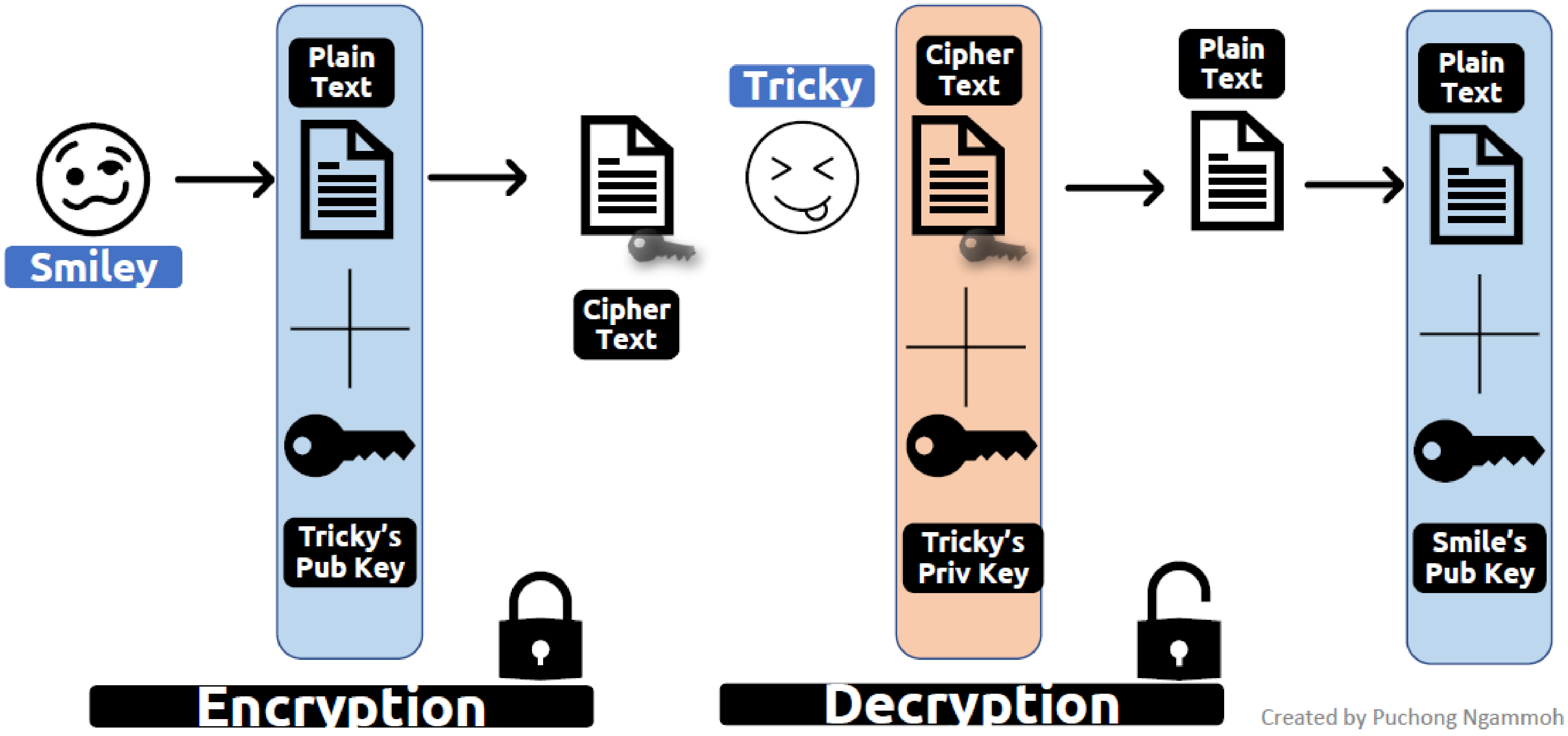
Scalability

Not scalable | scalable

Use

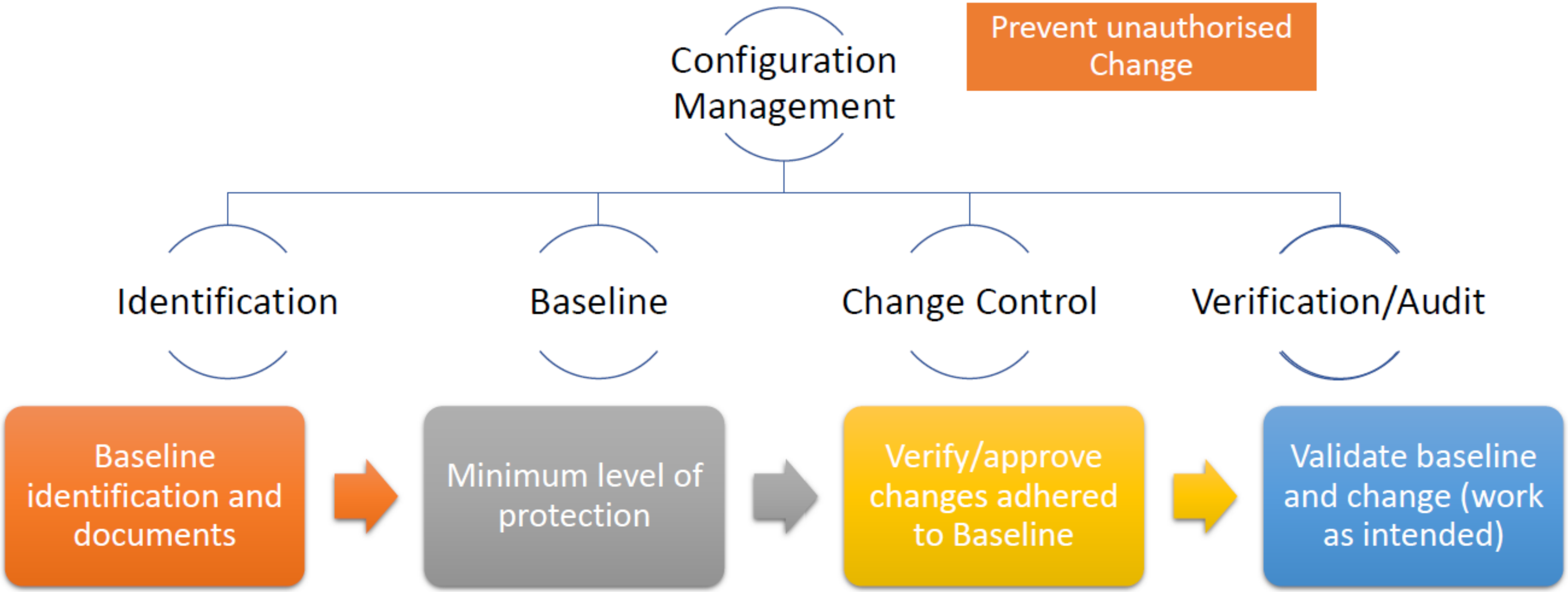
Storage/IPsec/TLS | Website/TLS/Access Control

Asymmetric Encryption



Created by Puchong Ngammoh CISSP-IS
CISM®| CCSK | CASP+ | CySA-

System Hardening



Configuration Management

Prevent unauthorised Change

Identification

Baseline

Change Control

Verification/Audit

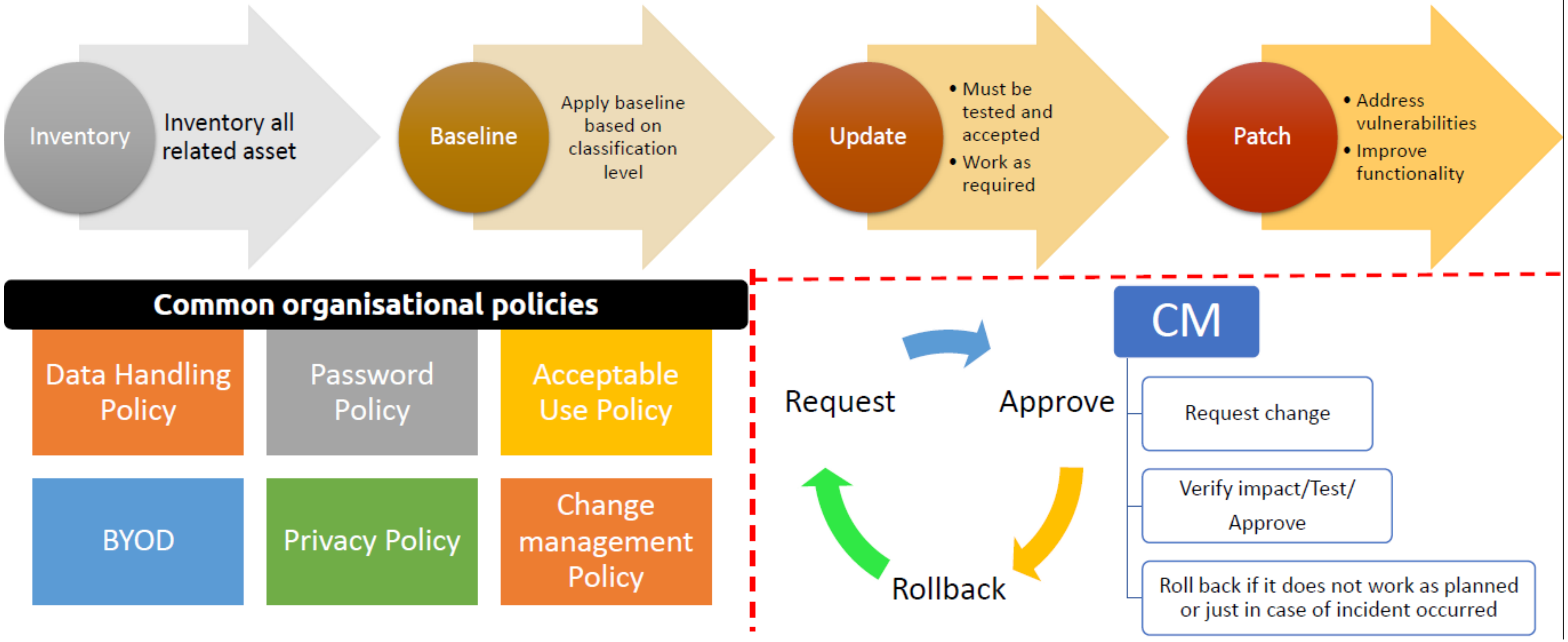
Baseline identification and documents

Minimum level of protection

Verify/approve changes adhered to Baseline

Validate baseline and change (work as intended)

Change Management Overview



Inventory

Inventory all related asset

Baseline

Apply baseline based on classification level

Update

- Must be tested and accepted
- Work as required

Patch

- Address vulnerabilities
- Improve functionality

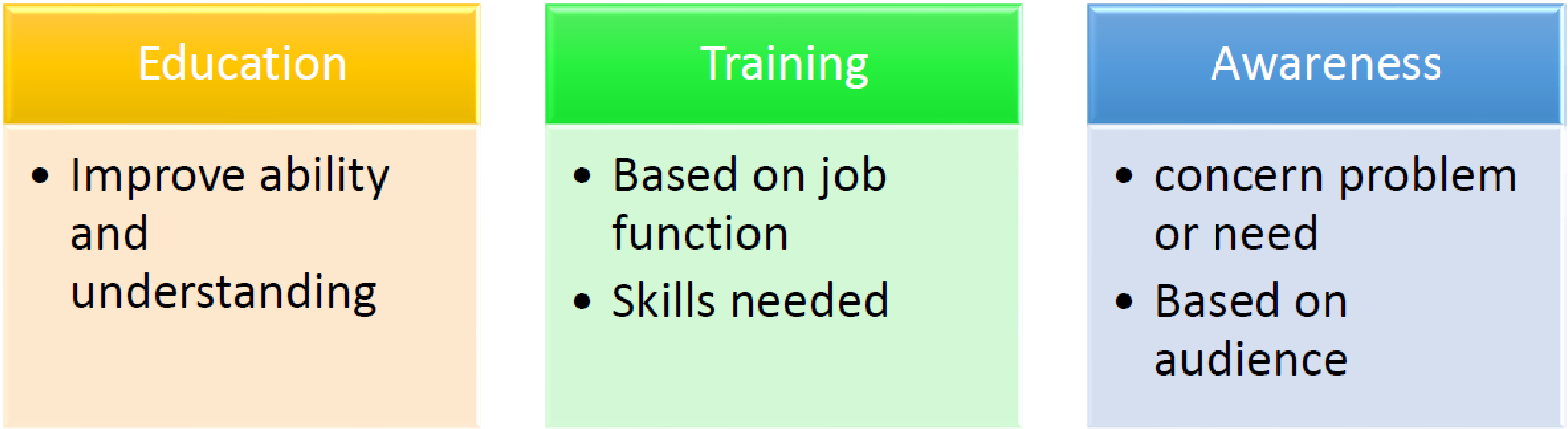
Common organisational policies

- Data Handling Policy
- Password Policy
- Acceptable Use Policy
- BYOD
- Privacy Policy
- Change management Policy

CM

- Request change
- Verify impact/Test/ Approve
- Roll back if it does not work as planned or just in case of incident occurred

Security Awareness



Education

- Improve ability and understanding

Training

- Based on job function
- Skills needed

Awareness

- concern problem or need
- Based on audience

To ensure understanding of individual expectation based on “Role and Responsibilities”