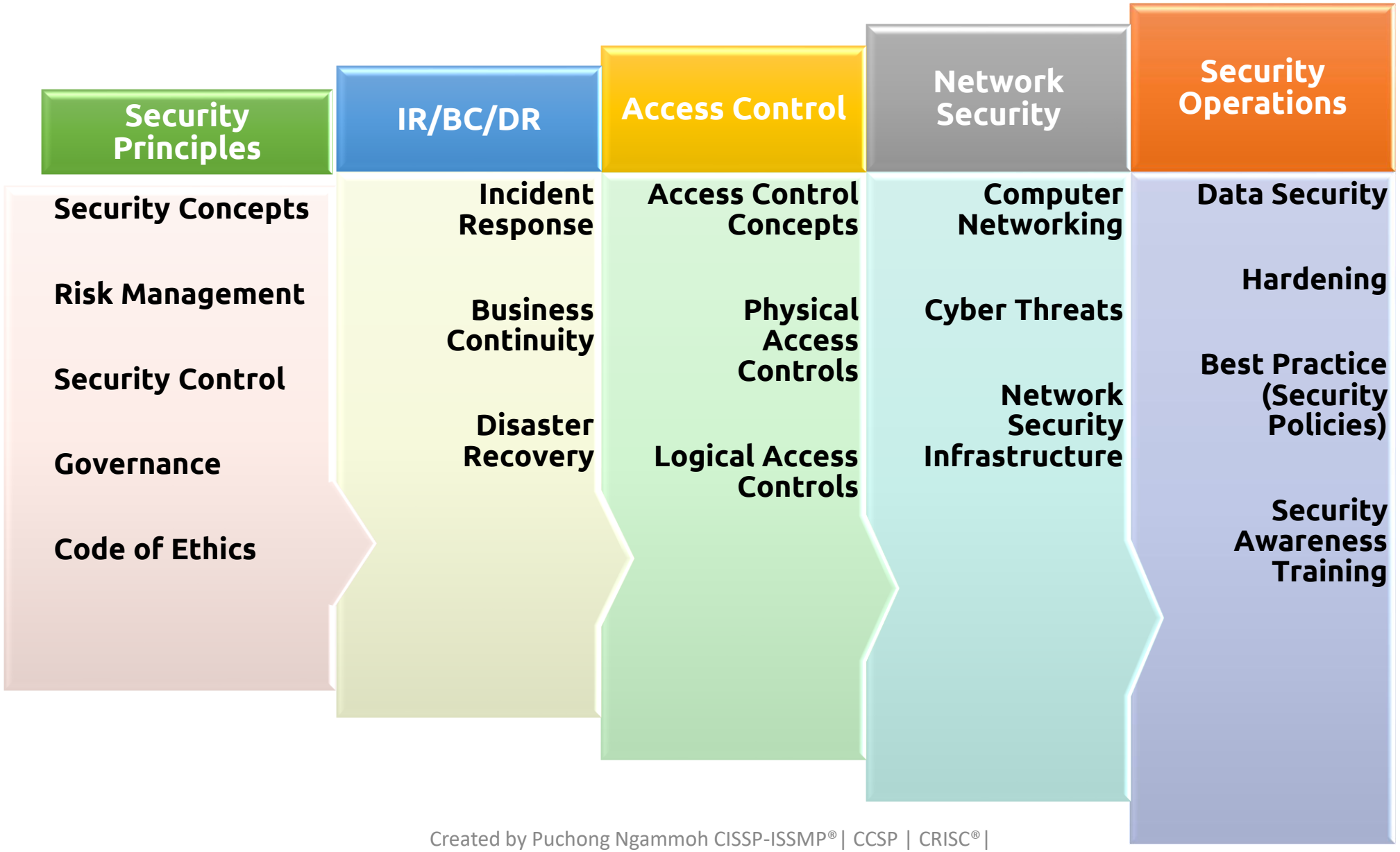
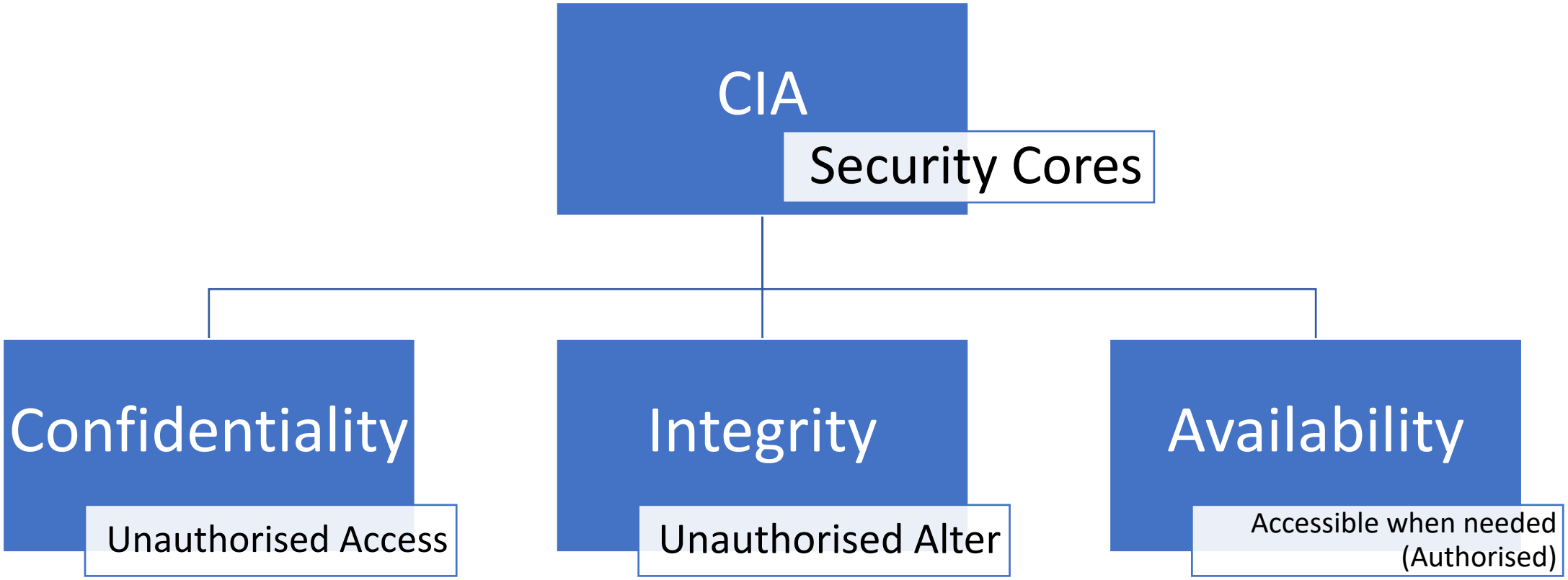
Last Minute Reminder CC – Certified in Cyber Security

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


Security Principles
IR/BC/DR
Access Control
Network Security
Security Operations
Security Concepts
Risk Management
Security Control
Governance
Code of Ethics
Incident Response
Business Continuity
Disaster Recovery
Access Control Concepts
Physical Access Controls
Logical Access Controls
Computer Networking
Cyber Threats
Network Security Infrastructure
Data Security
Hardening
Best Practice (Security Policies)
Security Awareness Training

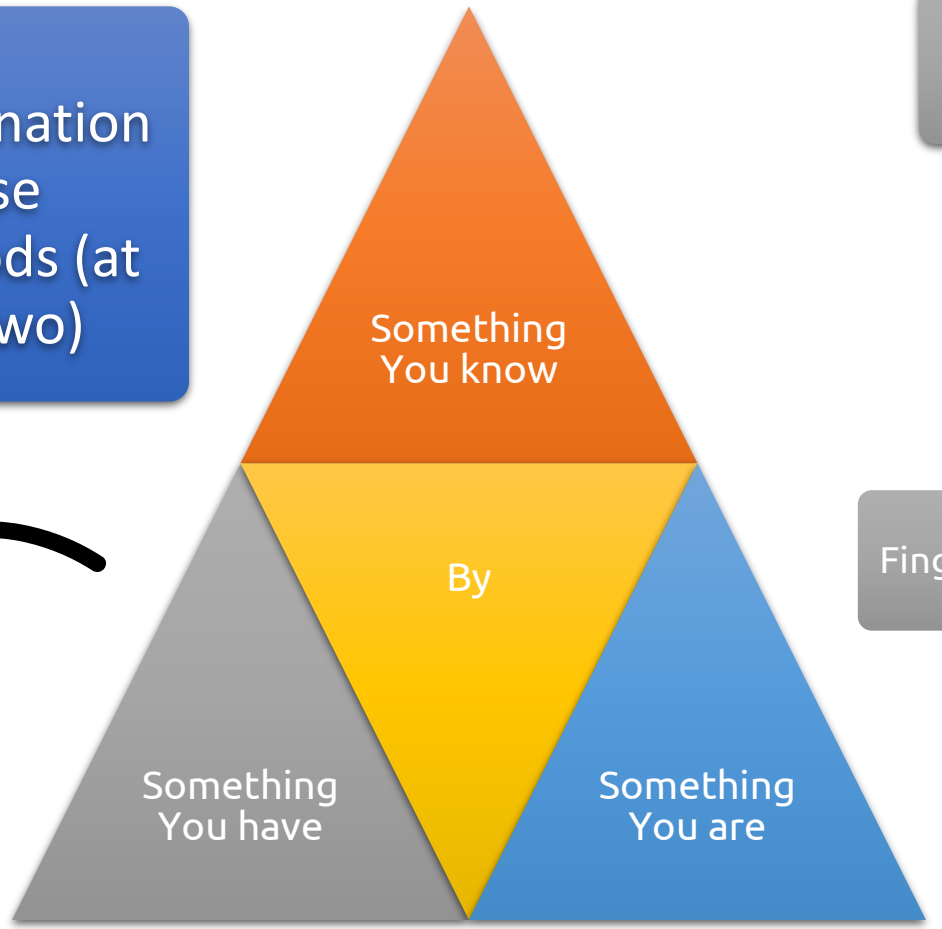
Security Principles



Authentication

SFA Use one of these methods

MFA Use combination of these methods (at least two)



Passwords

Paraphrases

Pin Number

Key Card

Badge

Tokens

Fingerprint

Face

Retina

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

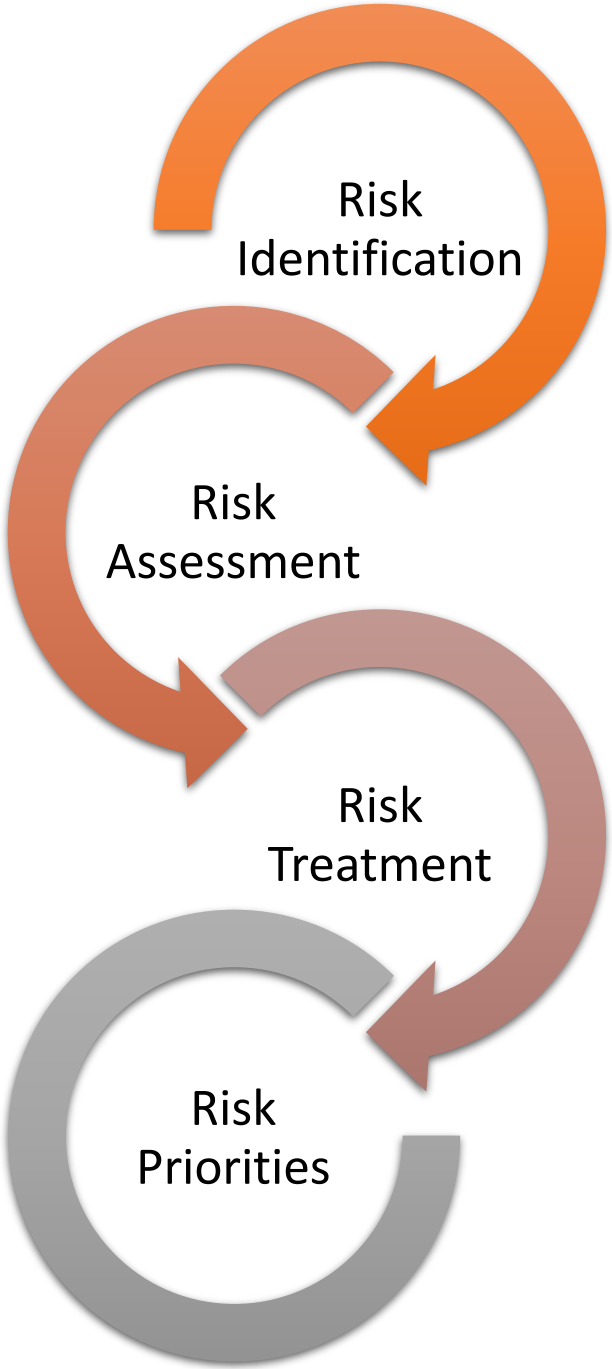
- Threat / Risk Posed to organisation
- People/Asset/Service

Risk Assessment

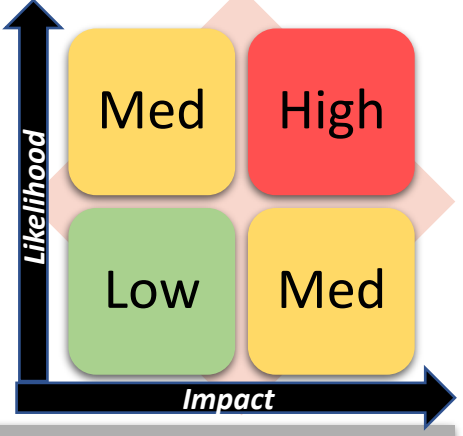
- Estimate/prioritise
- Likelihood x Impact
  - Qualitative (H/M/L)
  - Quantitative ($)

Risk treatment

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



Risk Priorities / Risk Tolerance



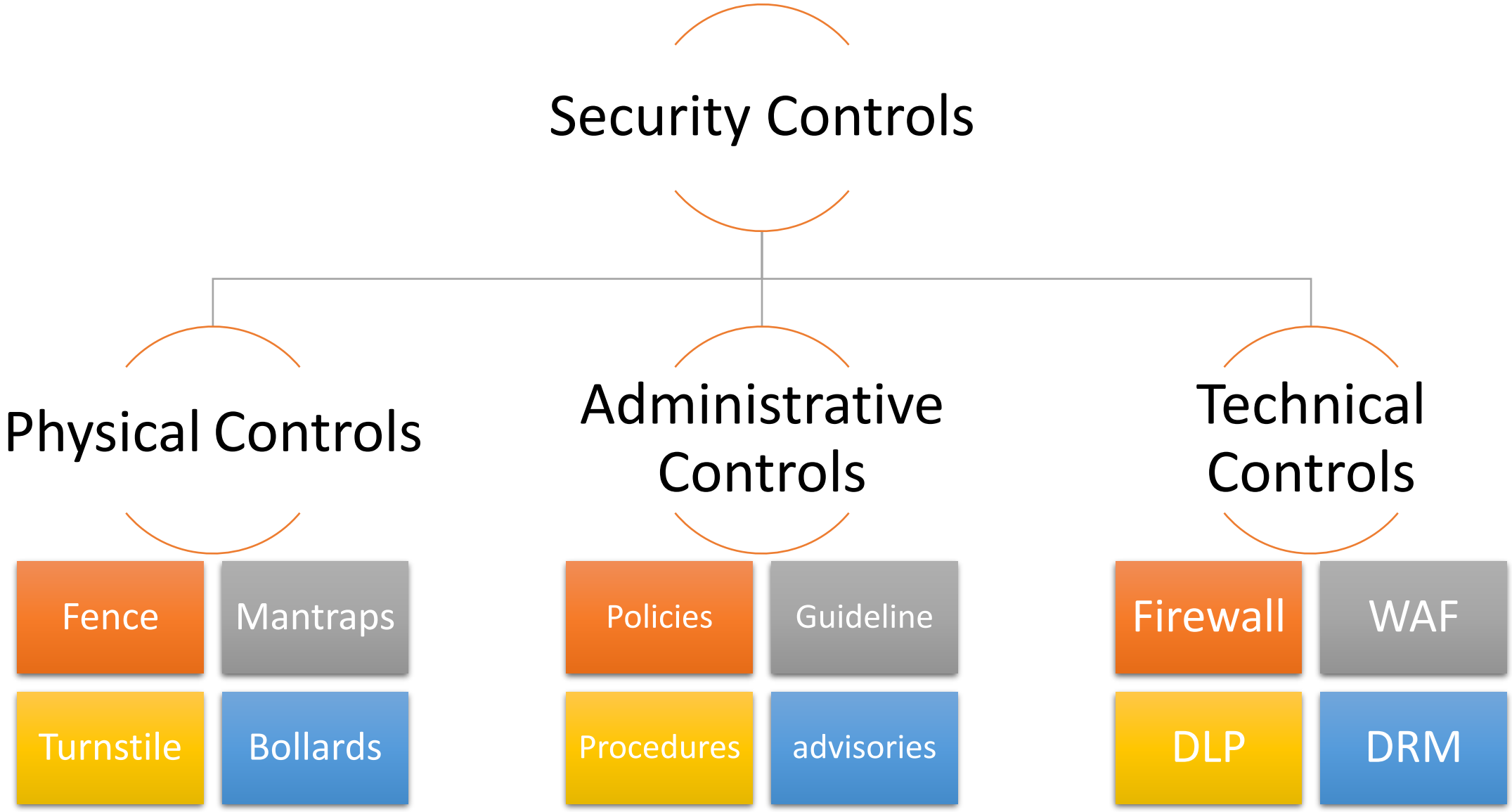
Risk Priorities

- 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)

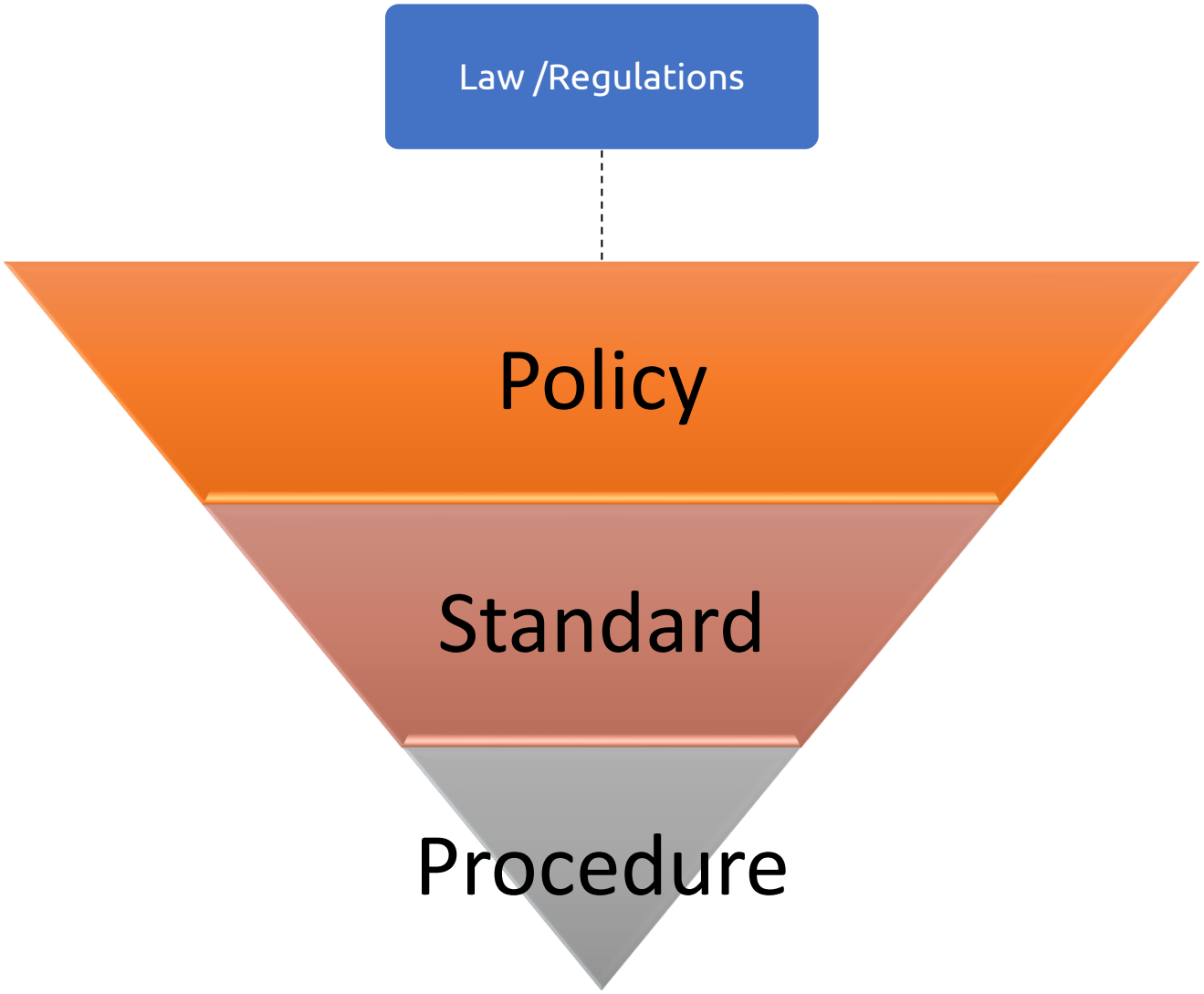
- AUP
- Access Control Policy

Standard (may include technical controls)

- ISO
- NIST
- PCI DSS

Procedures (Day-to-Day Operations)

- Special Tasks
- routine activities



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

Goal of IR

- To reduce impact of incident

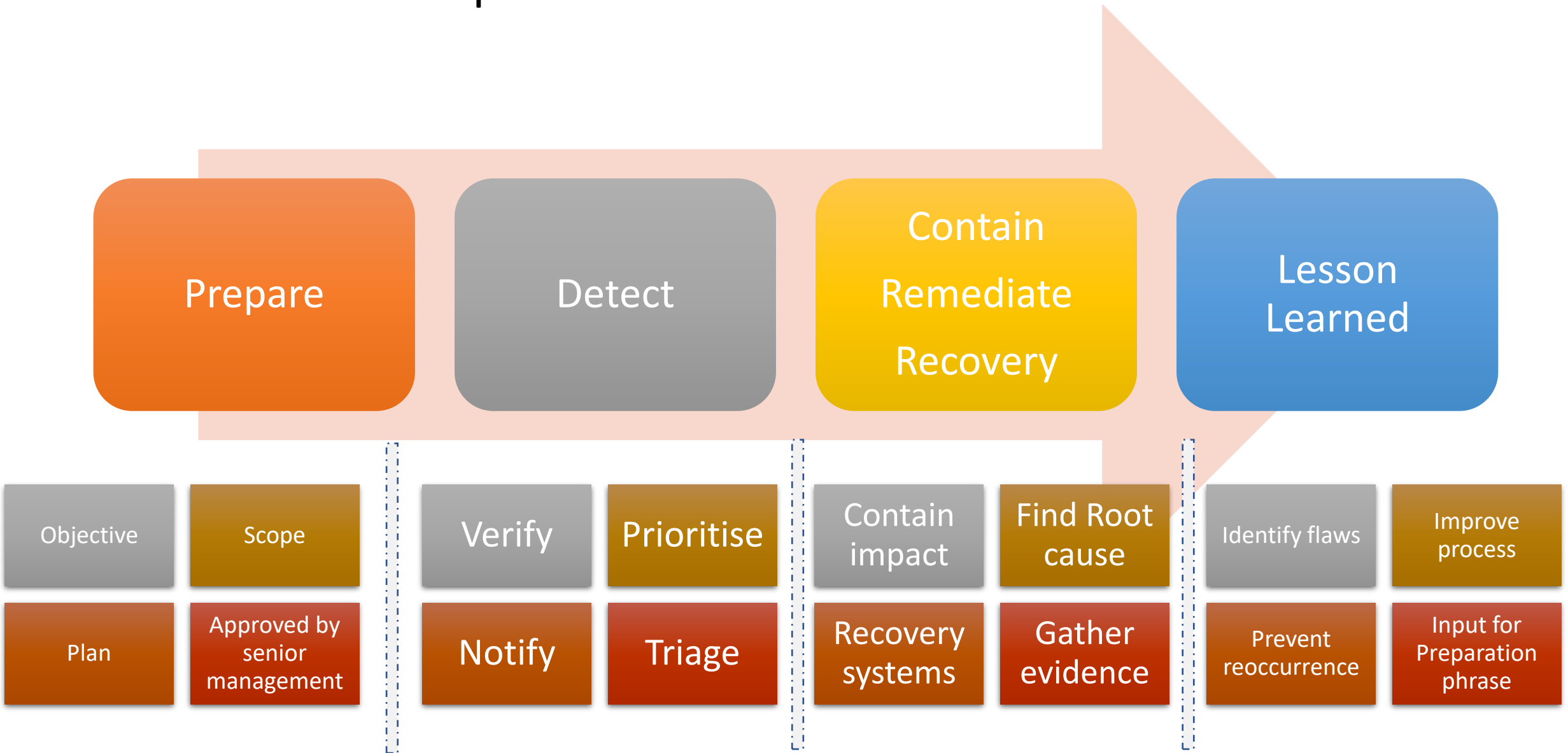
Goal of BC

- 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



Business Continuity

BCP Team

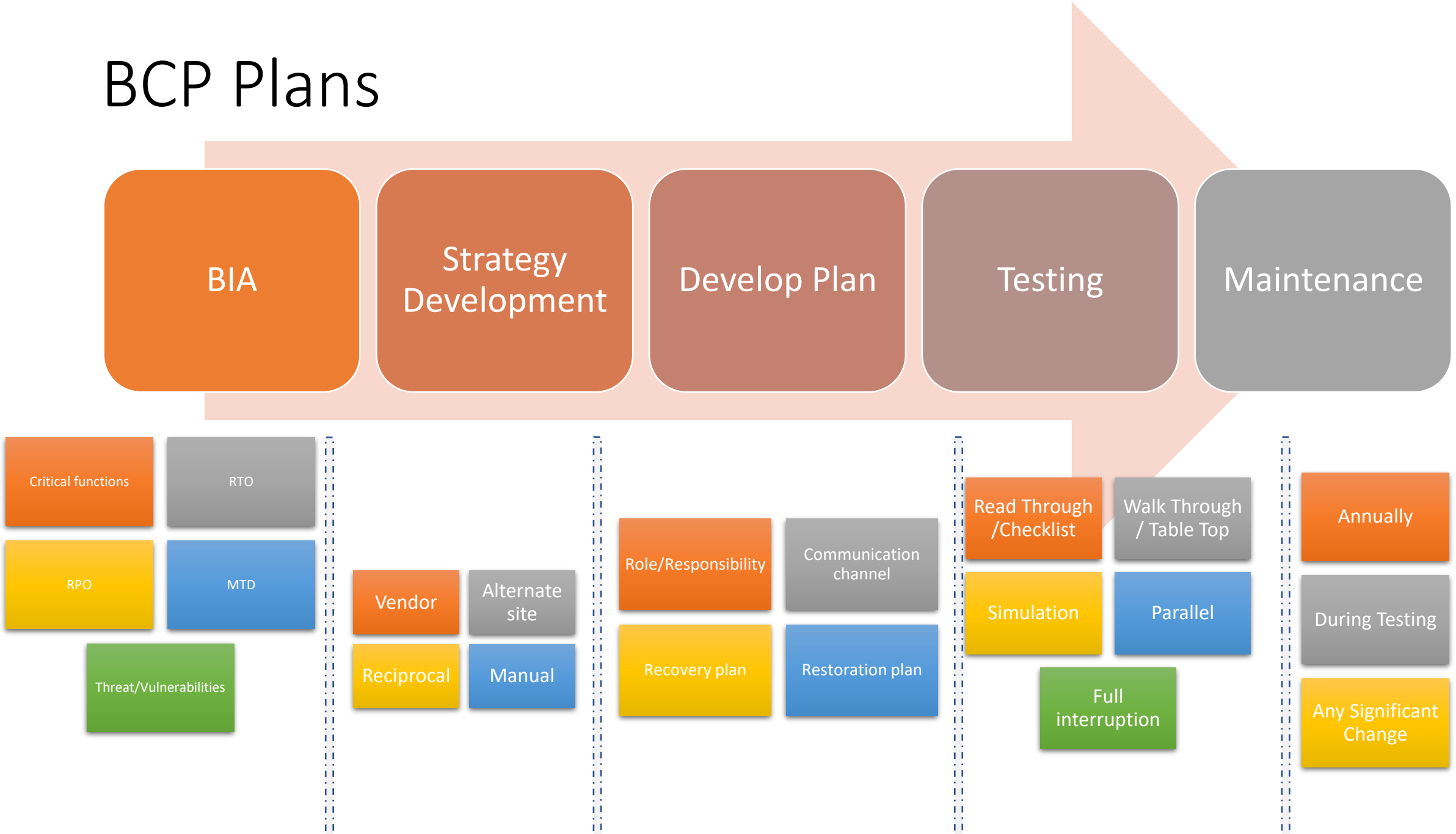
Response procedures (1st /2nd)

Communication (Call tree)

BCP Announcement (Who/When)

External Communication (emergency services, customers, vendors)

BCP Plans


BIA
Strategy Development
Develop Plan
Testing
Maintenance
Critical functions
RTO
RPO
MTD
Threat/Vulnerabilities
Vendor
Alternate site
Reciprocal
Manual
Role/Responsibility
Communication channel
Recovery plan
Restoration plan
Read Through /Checklist
Walk Through / Table Top
Simulation
Parallel
Full interruption
Annually
During Testing
Any Significant Change

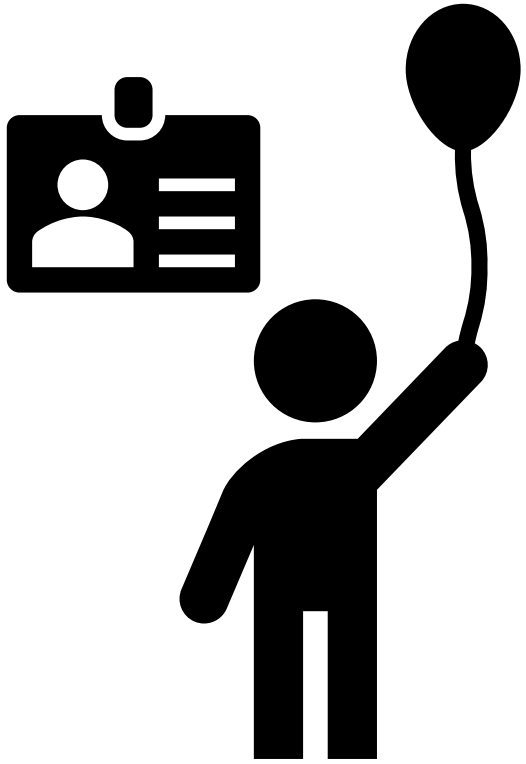
Disaster Recovery Plan

Public relation

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

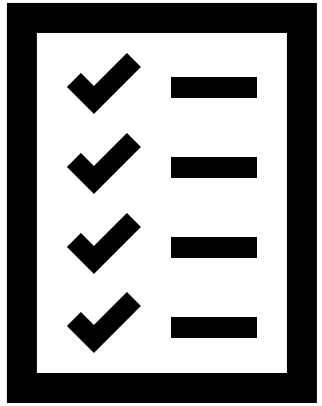
Checklist

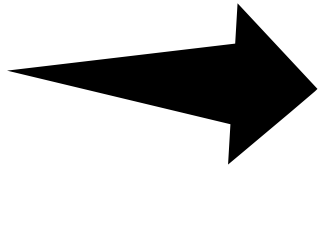
- Will help prioritising step and procedures during crisis occurred

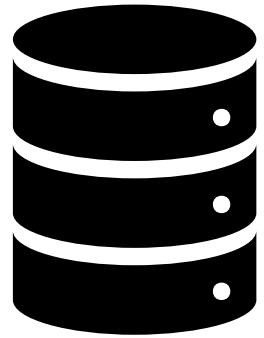


Rules

- Access Control list
- Allow/deny request







Objects

- Service/System requested by subject
- Passive

Subjects

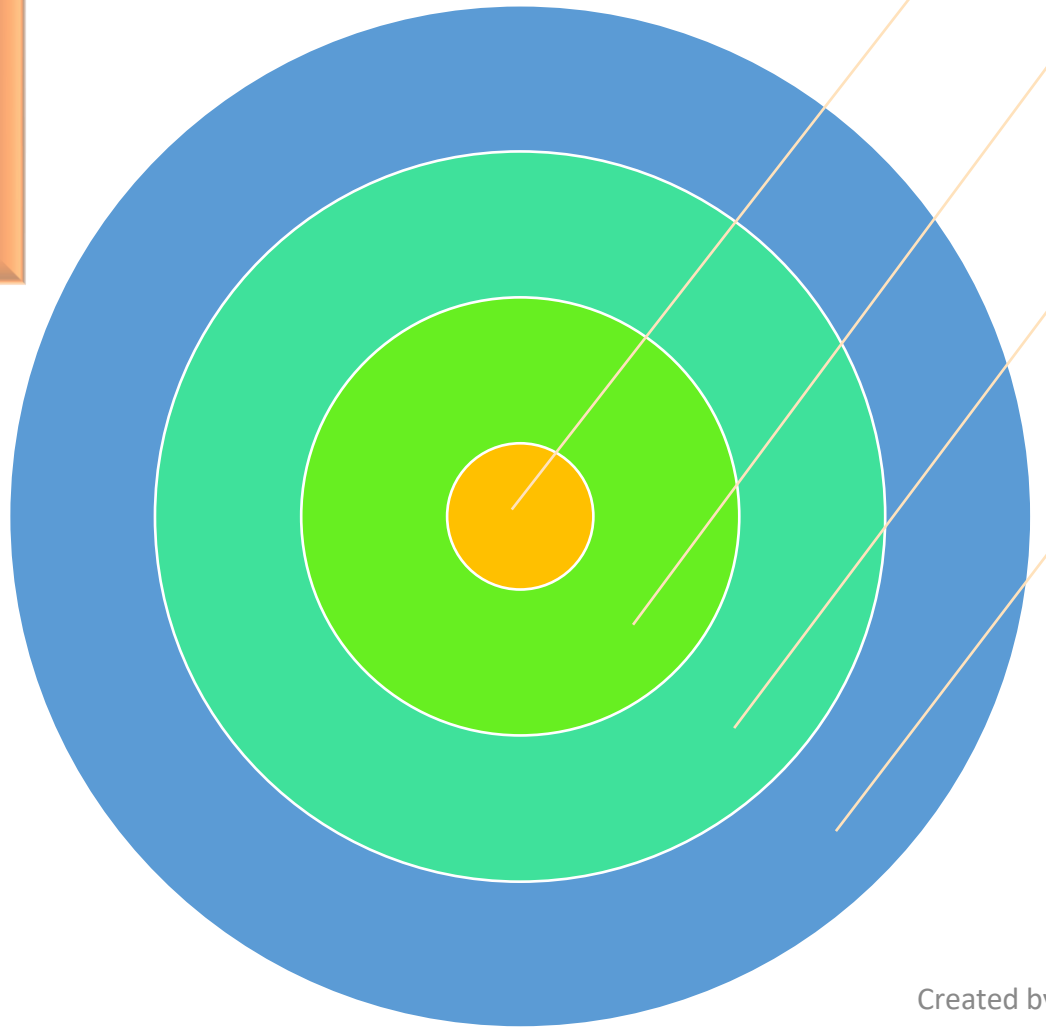
- Entity that request to access
- Active

Access Control

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

Defence in Depth

Multiple layers of controls for increasing security



Asset/ Objects

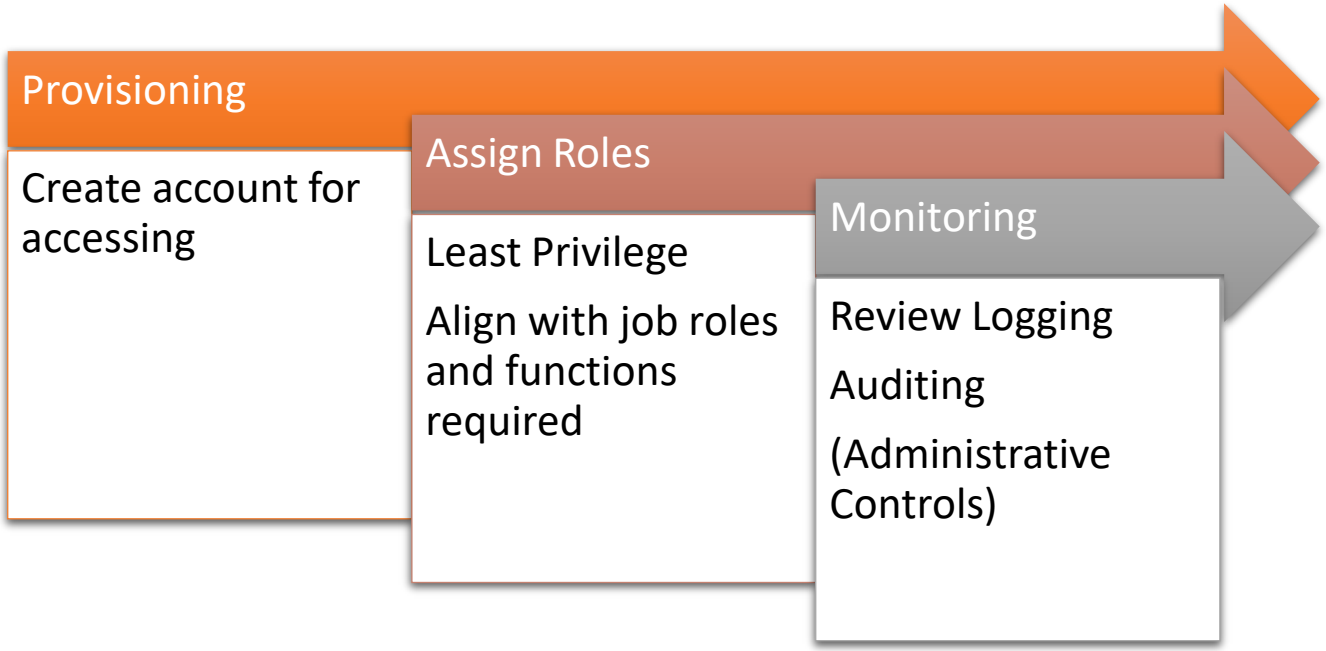
Administrative

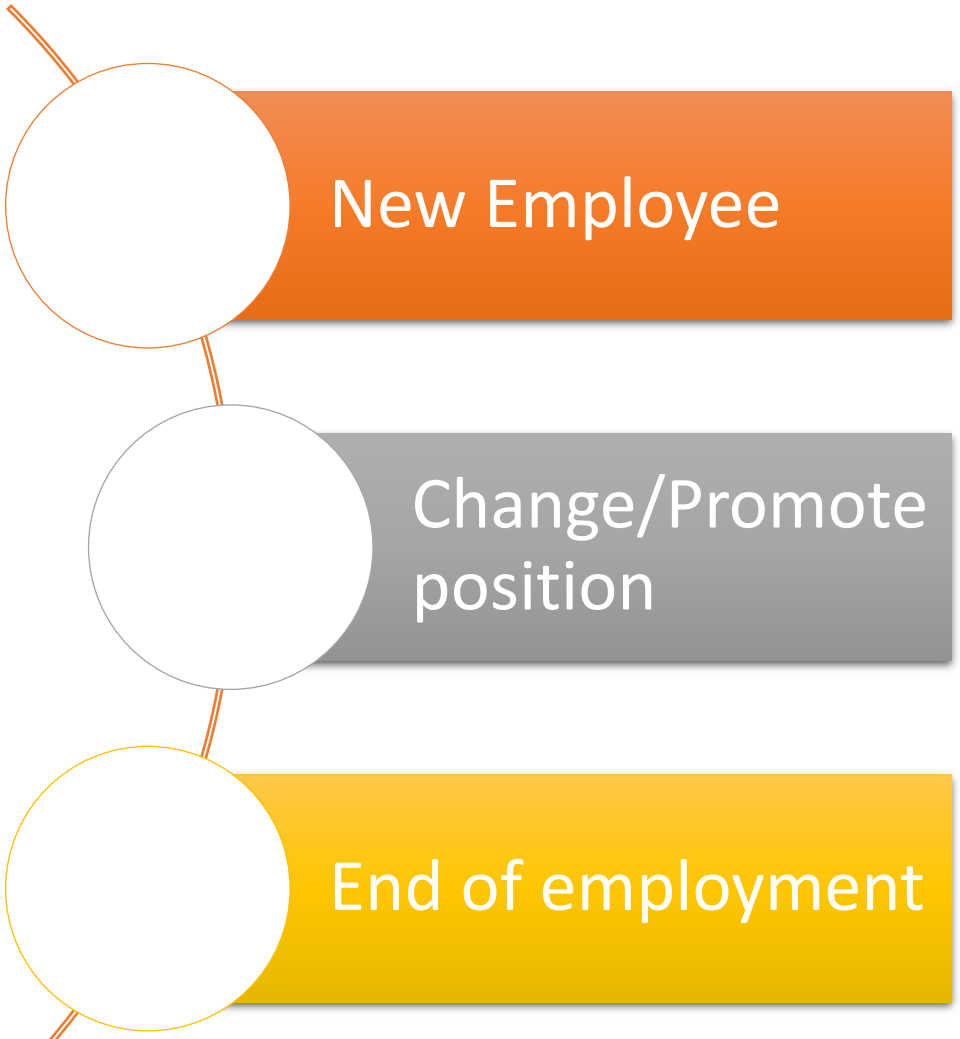
Technical

Physical

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

Privileged Access Management

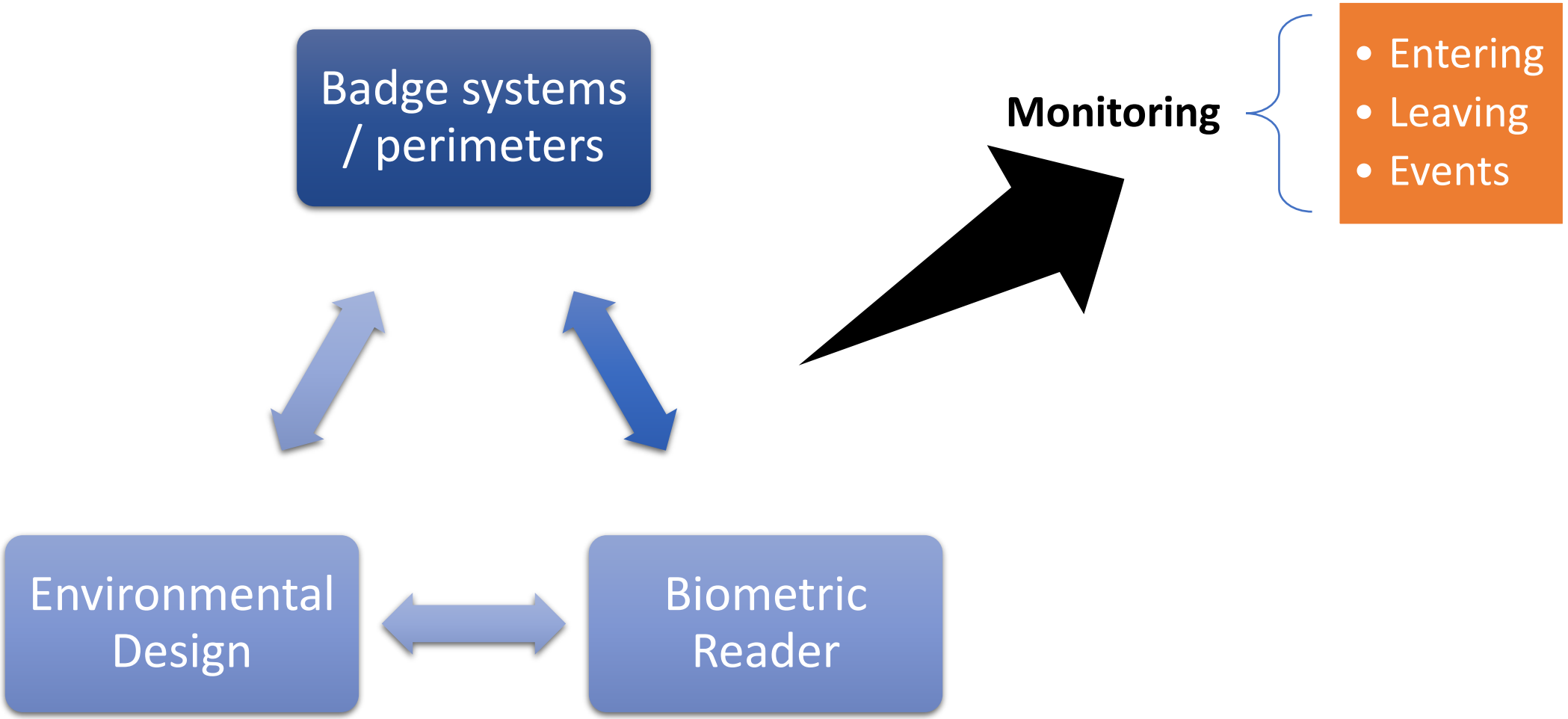




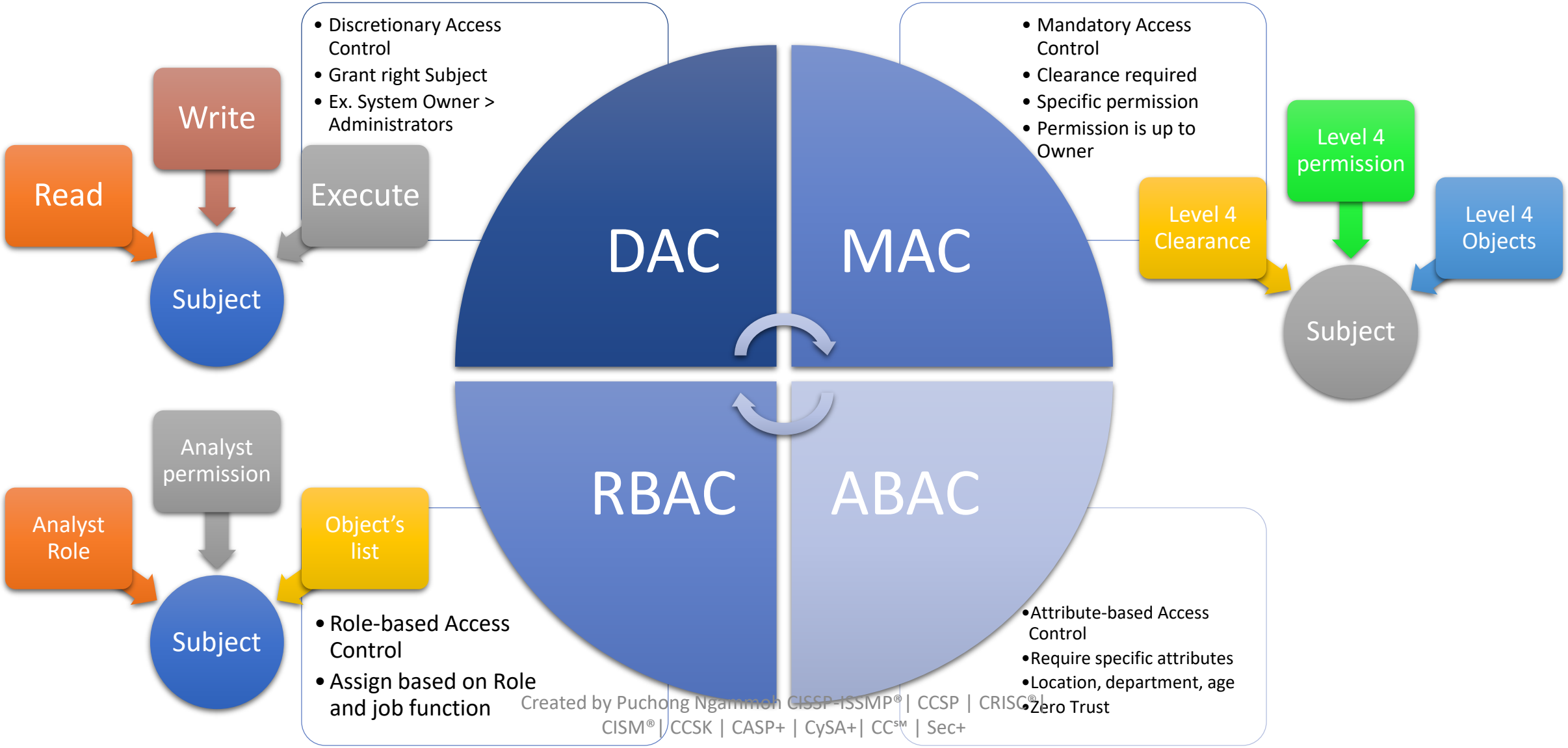
Segregation of Duties
- Separate related tasks and responsibilities

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

Access Control methods

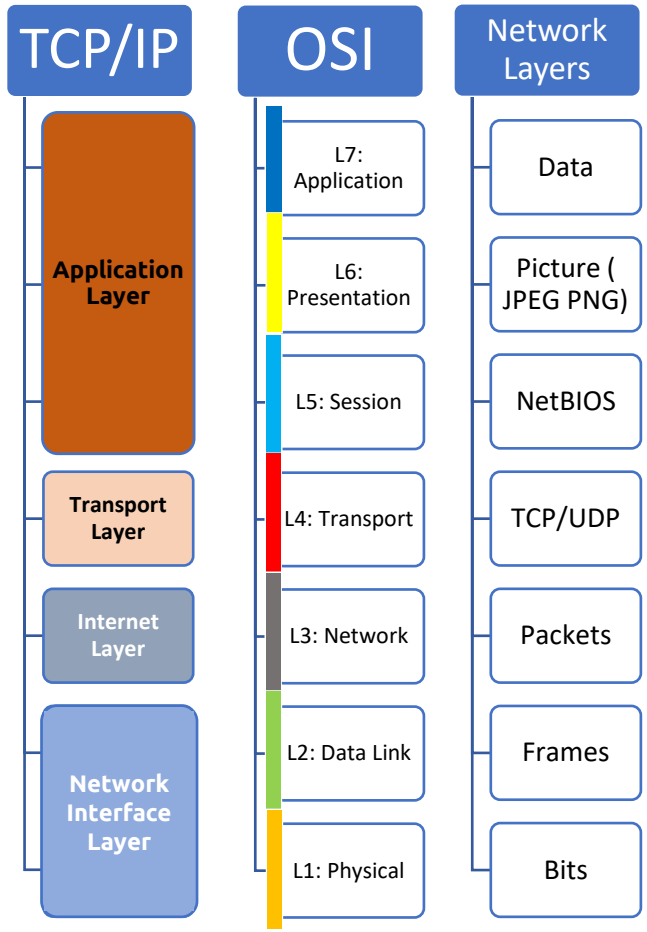


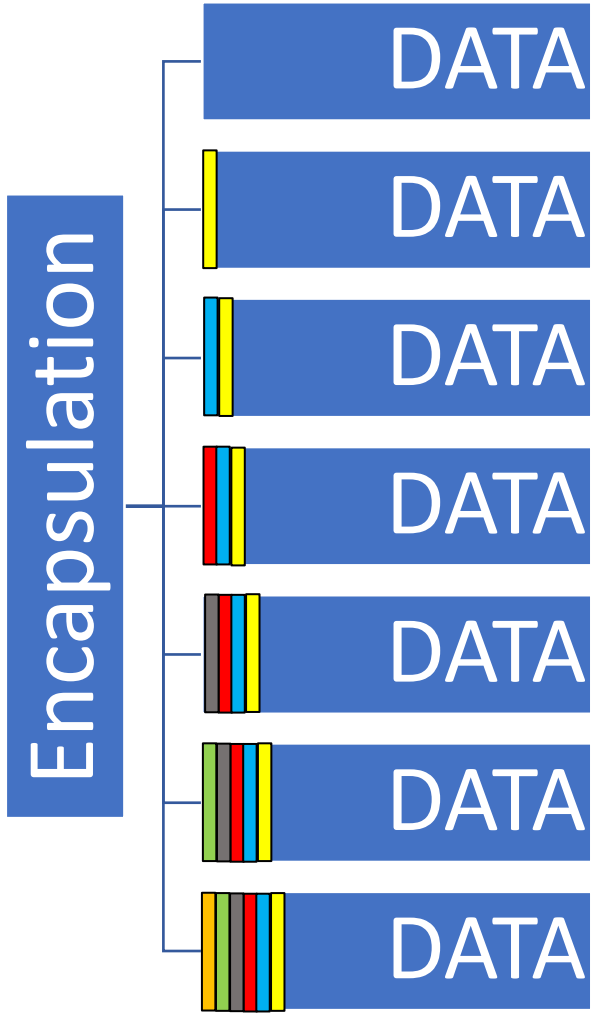
Access Control methods



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

Domain 4 : Networking





2^{32} **IPV4**

Network Address

192.168.1 .1

Host Address

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

127.0.0.1 Loopback

fc00:: to fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Internal Address

2^{128} **IPV6**

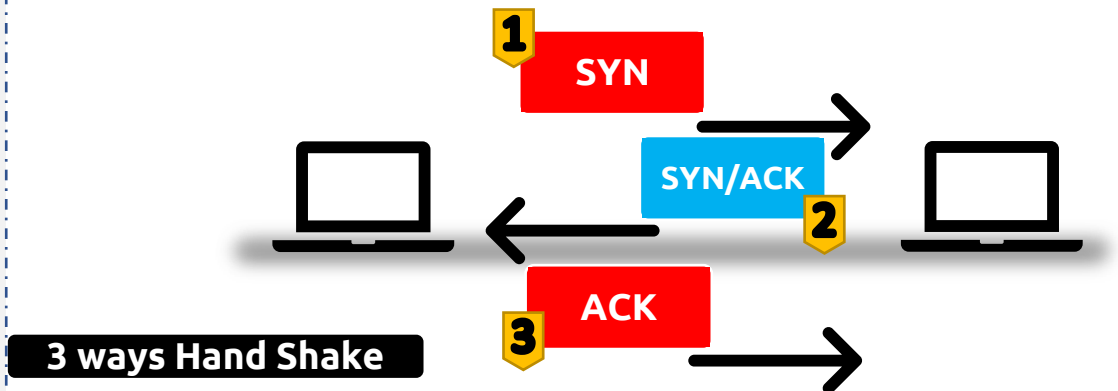
Created by Puchong Ngammoh CISSP-ISSMP® | CCSP | CRISC® | CISM® | CCSK | CASP+ | CySA+ | CC℠ | Sec+

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

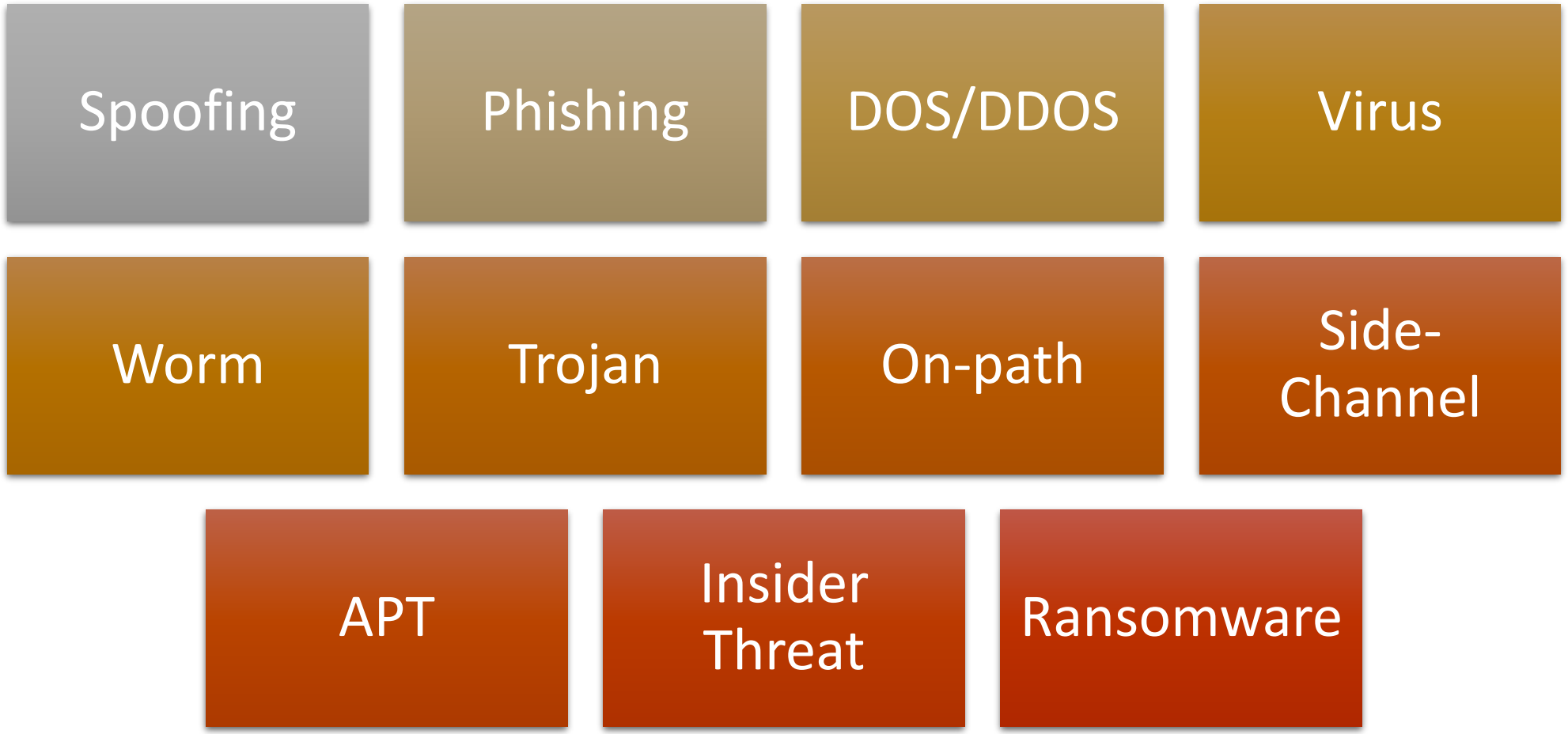
Fragment Attacks

Oversized Packet Attacks

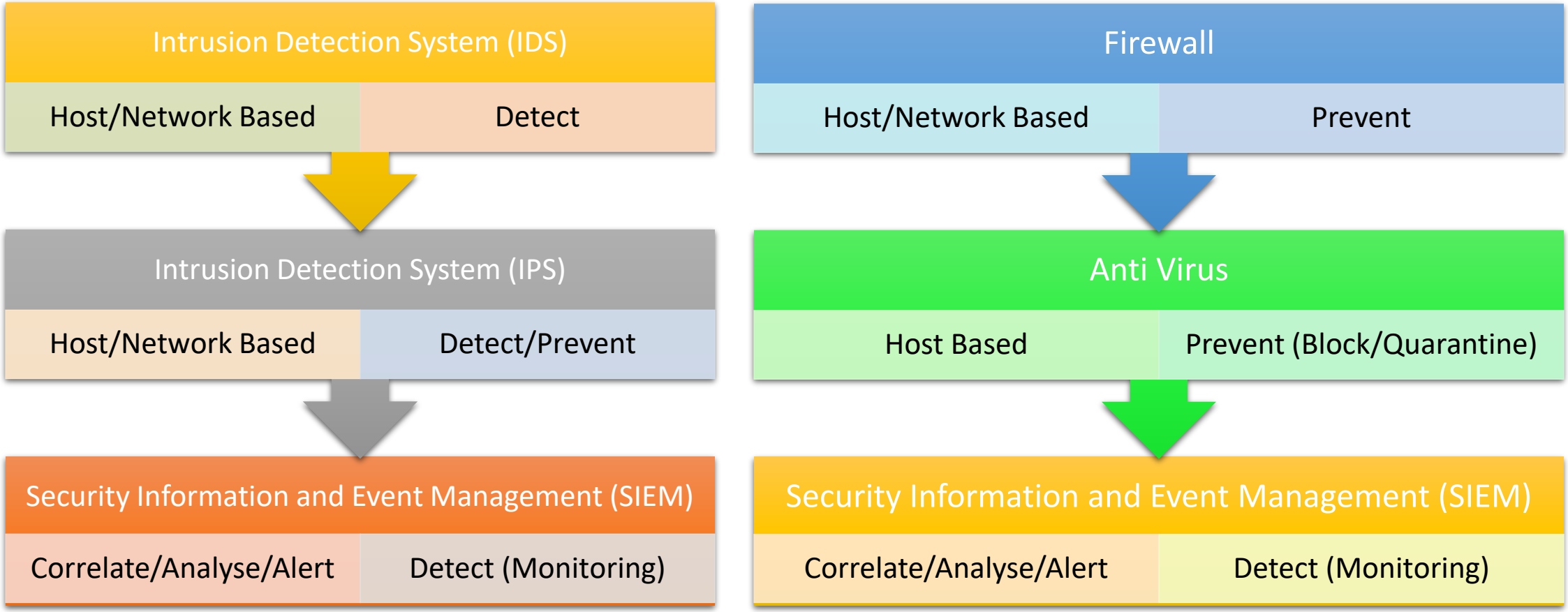
Spoofing Attacks

DOS/DDOS

Cyber Threat



Preventing/Detecting Threats



Data Centre Components

Closets

(Server/Network Connection / Wiring / Network devices)

HVAC

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

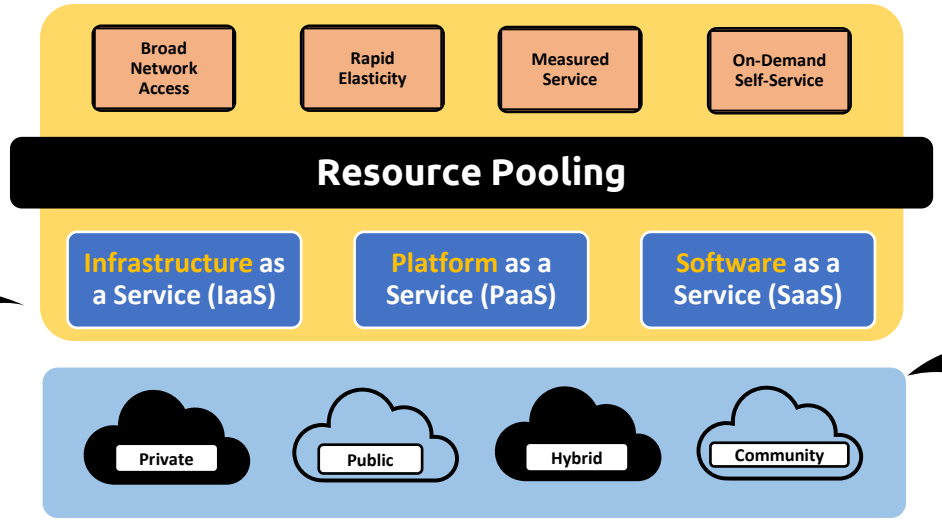
Power

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

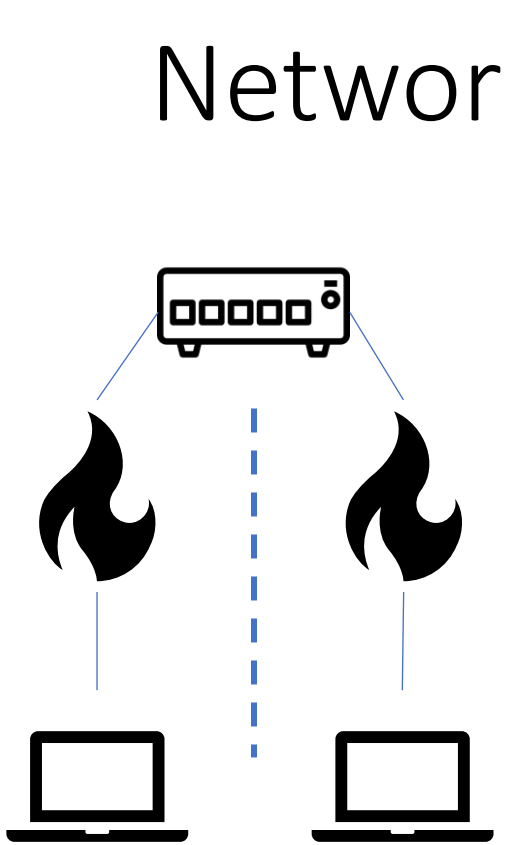
Private Cloud
- Solely own by one organisation using own resources

Public Cloud
- Shared resources with other tenants

Hybrid Cloud
- Combination of one or more cloud deployments

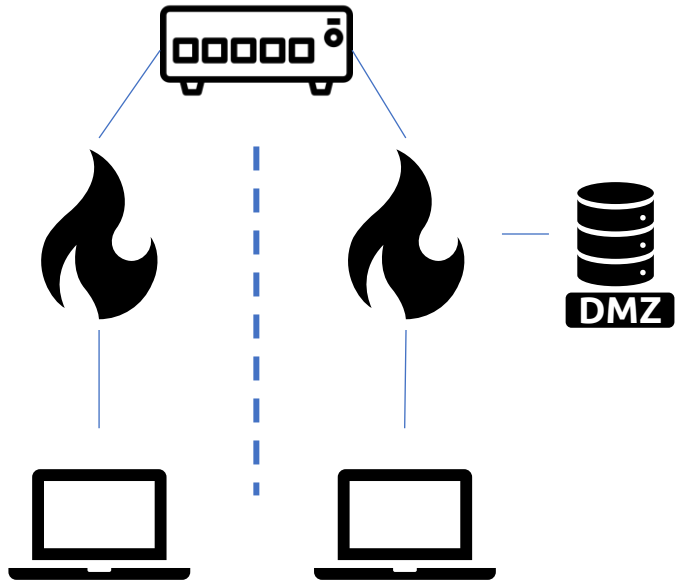
Community Cloud
- Affinity Group on same objectives

Network Designing



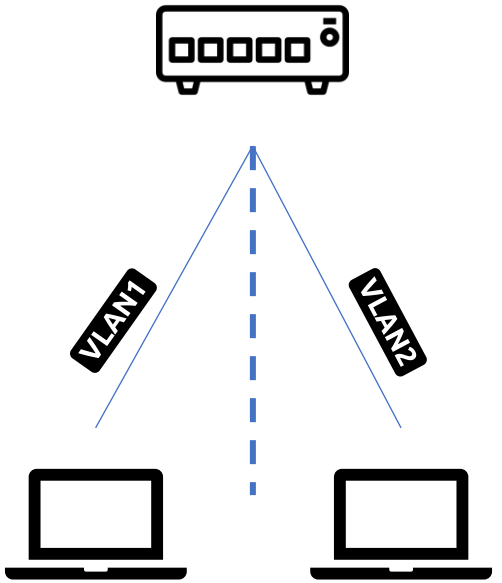
Network Segmentation

Isolated from all outside communications



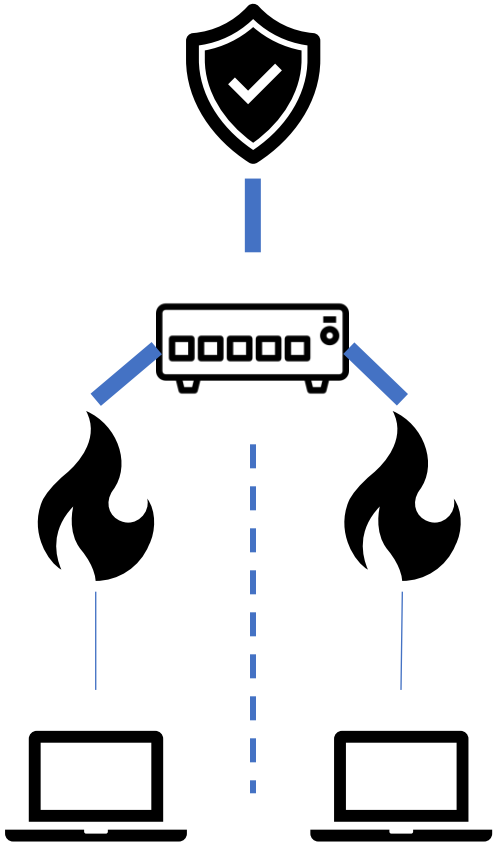
Demilitarised Zone (DMZ)

Isolated internet-facing zone



Virtual Local Area Network (VLAN)

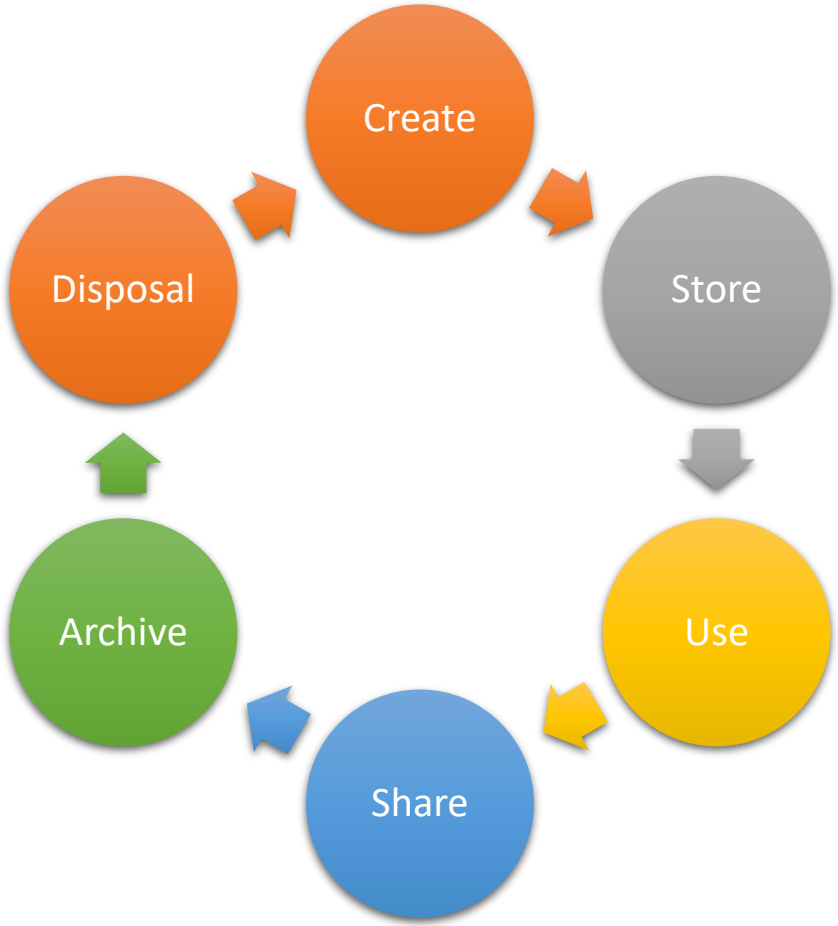
Isolated internal network



Virtual Private Network (VPN)

Secure communication in transit

Data Life cycle



Data Classification

- Data Owner
- Sensitivity

Labelling

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

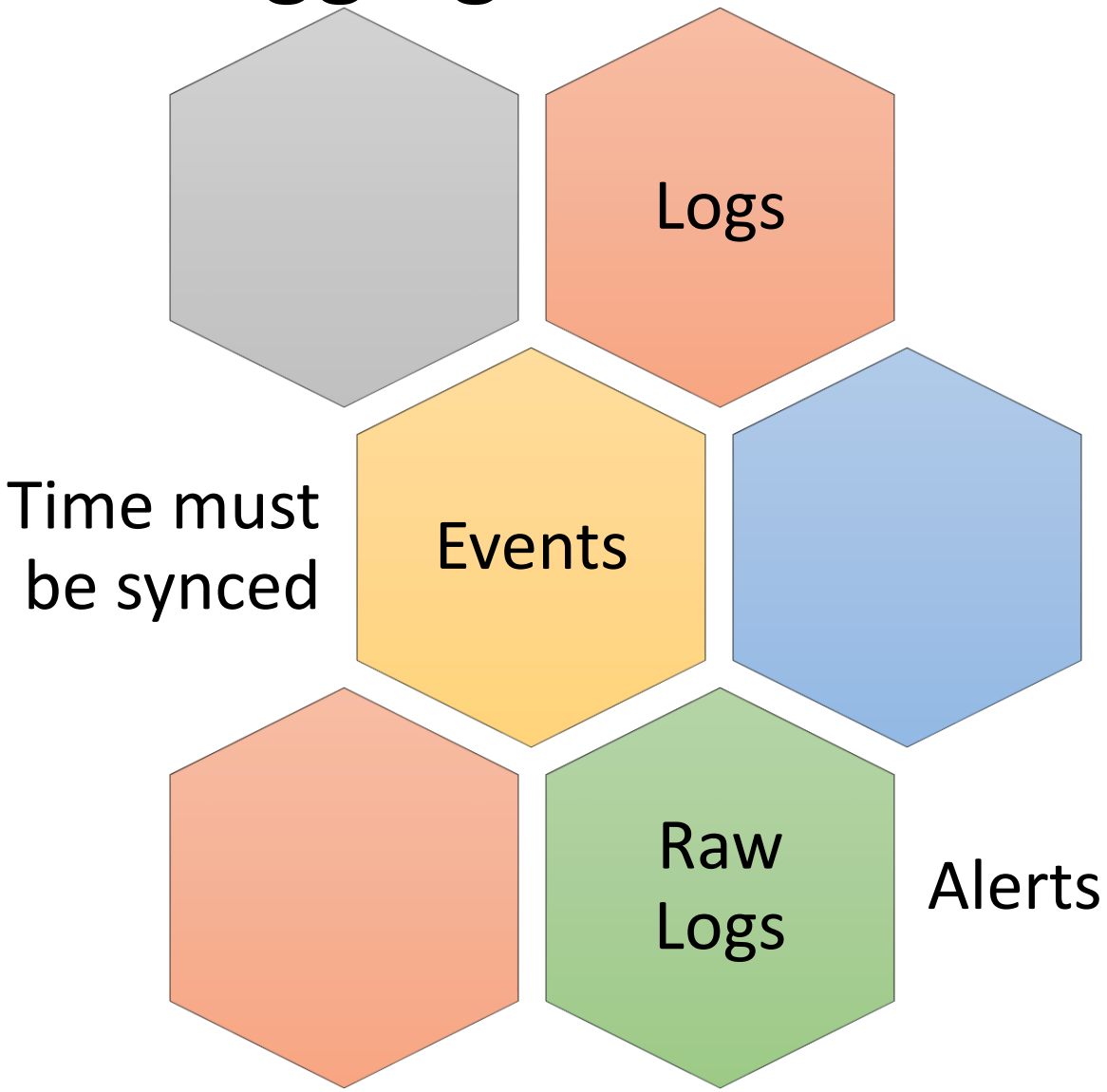
Data Retention

- 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



- USER Activities
- SYSTEM Activities
- Authentication
- Configuration Changes

Common Log Sources

Firewall

Network Devices

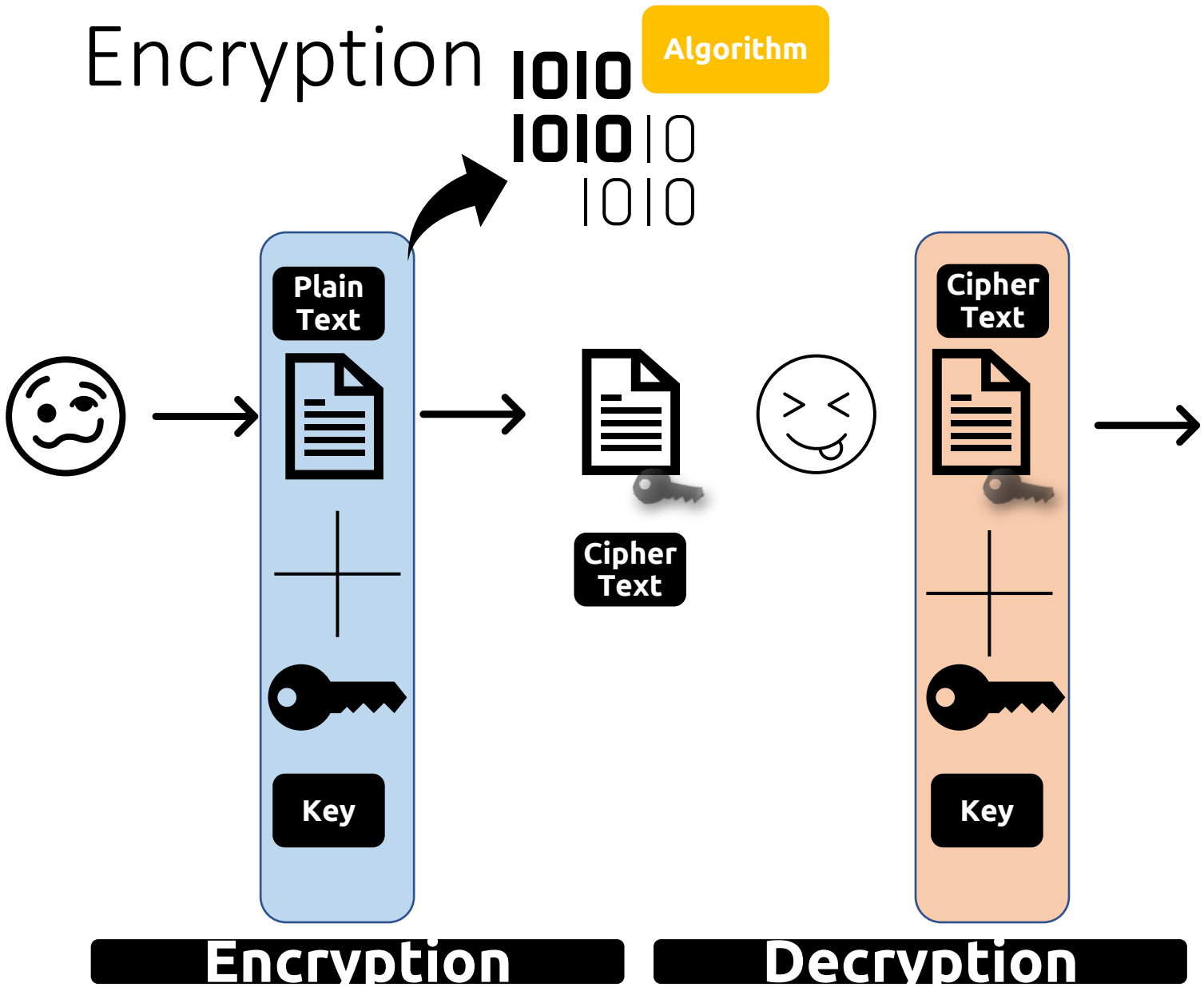
IDS/IPS

Anti Malware

Proxy

Threat Intelligence Feeds

Encryption



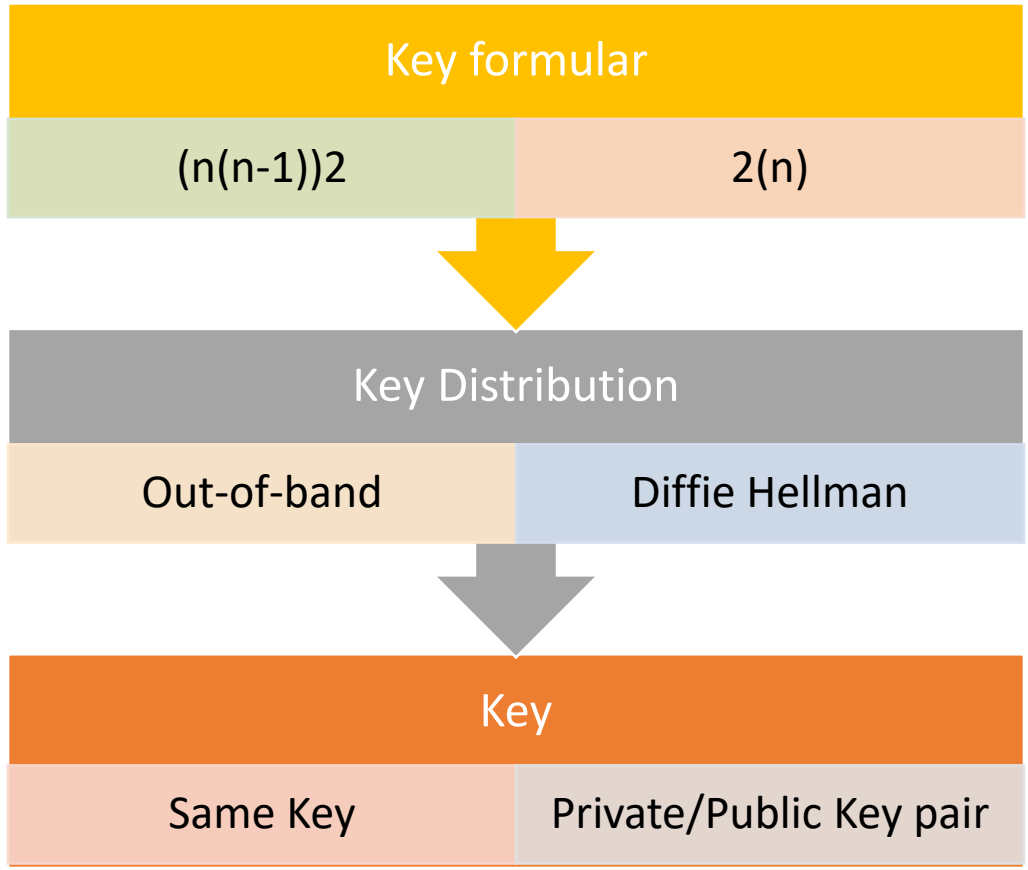
Hashing

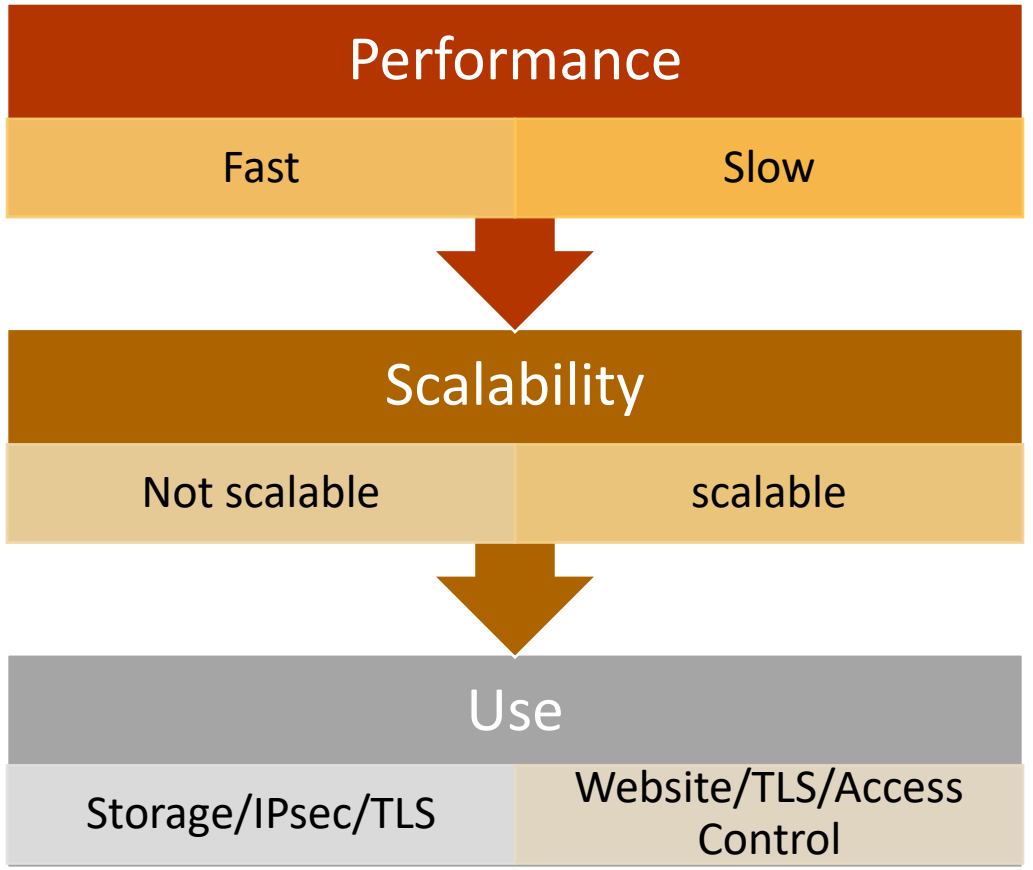
- 1-way
- Integrity Check
- Ensure that message is not altered

Digital Signature

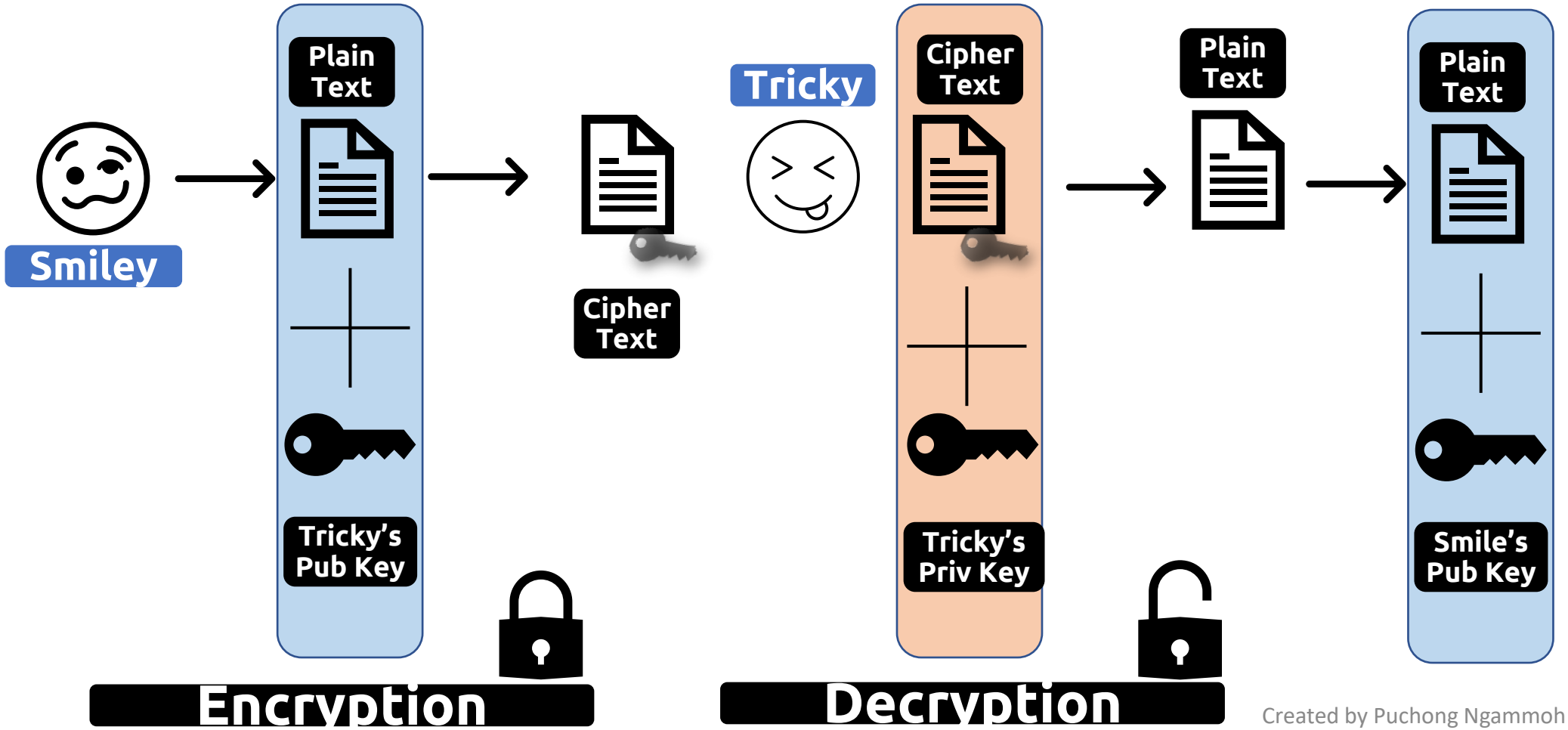
- Authenticity
- Non-repudiation
- Sign with private key of sender

Symmetric / Asymmetric



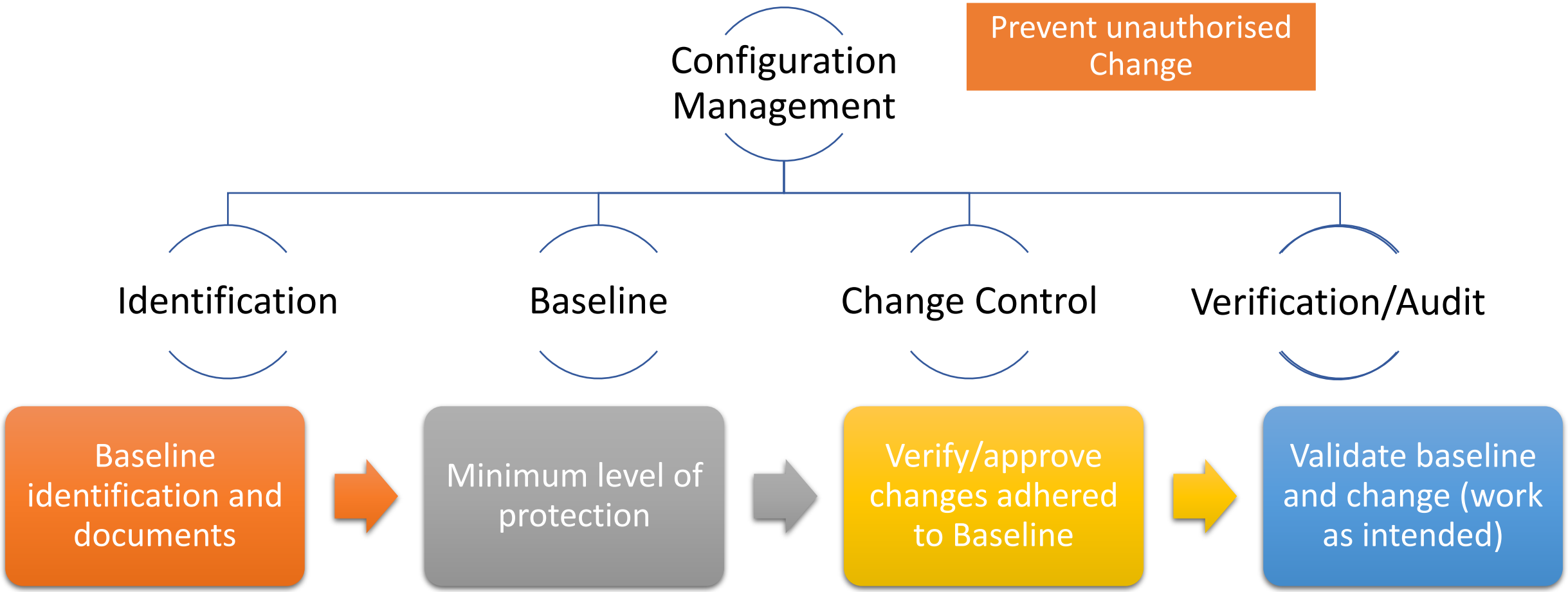


Asymmetric Encryption

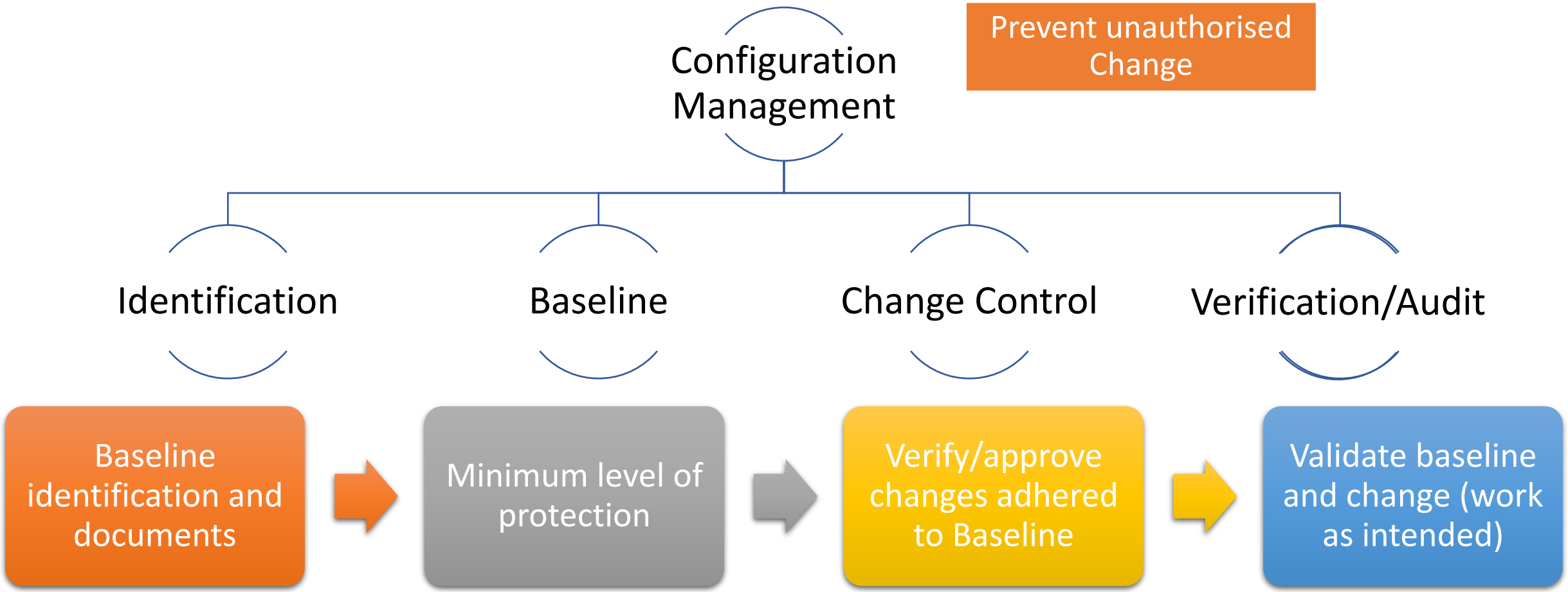


Created by Puchong Ngammoh CISSP-ISSMP®| CCSP | CRISC®| CISM®| CCSK | CASP+ | CySA+| CC℠ | Sec+

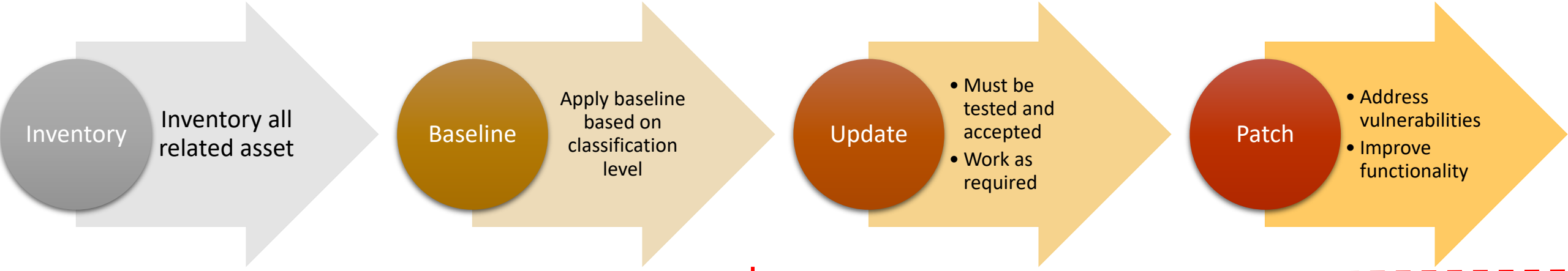
System Hardening



System Hardening

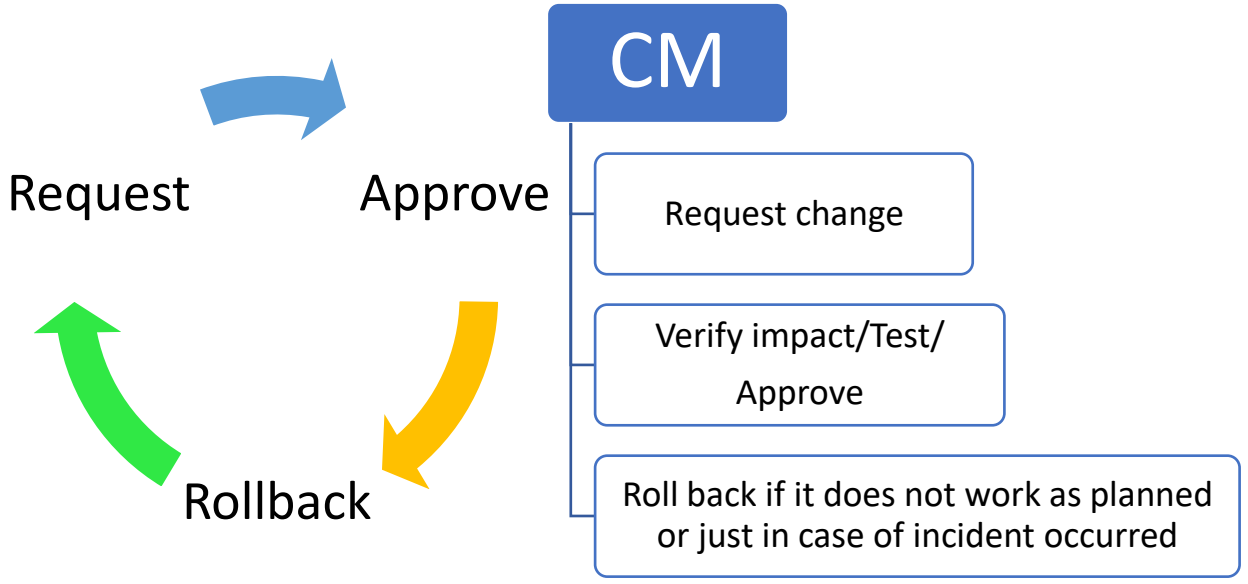


Change Management Overview



Common organisational policies

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



Security Awareness

Education	Training	Awareness
• Improve ability and understanding	• Based on job function • Skills needed	• concern problem or need • Based on audience

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