CMP4103

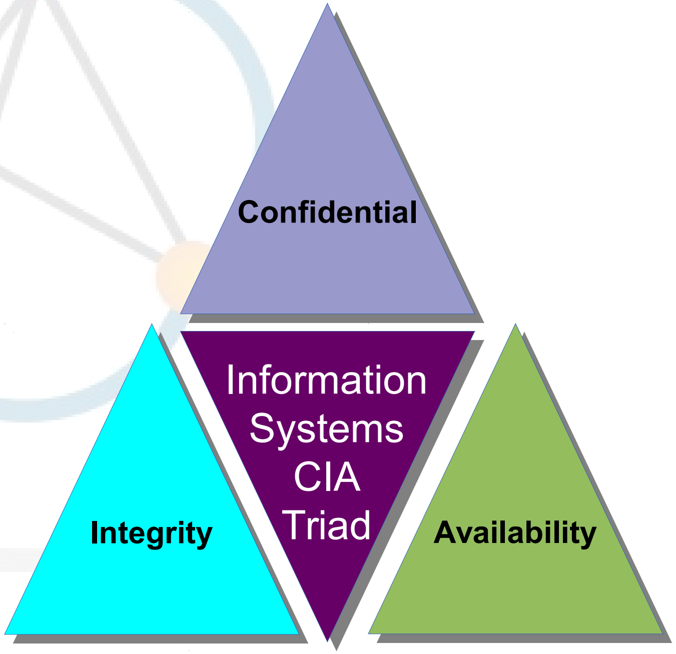
Computer Systems and Network Security Revision

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

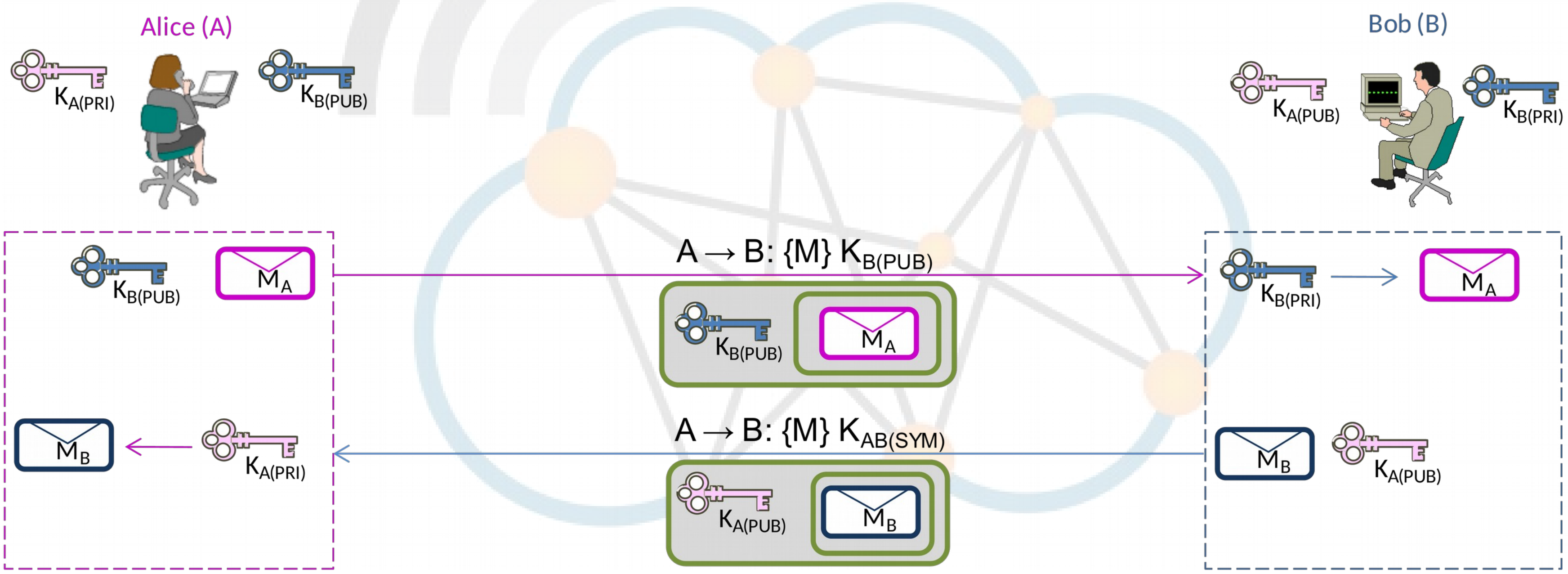
Cryptography

- CIA Triad principles
- Hash and encryption methods
  - Data Encryption Standard (DES)
  - Double DES (DDES)
  - Triple DES (TDES)
  - Advanced Encryption Standard (AES).
  - Message-Digest algorithm (MD5)
  - Secure Hash Algorithm (SHA)

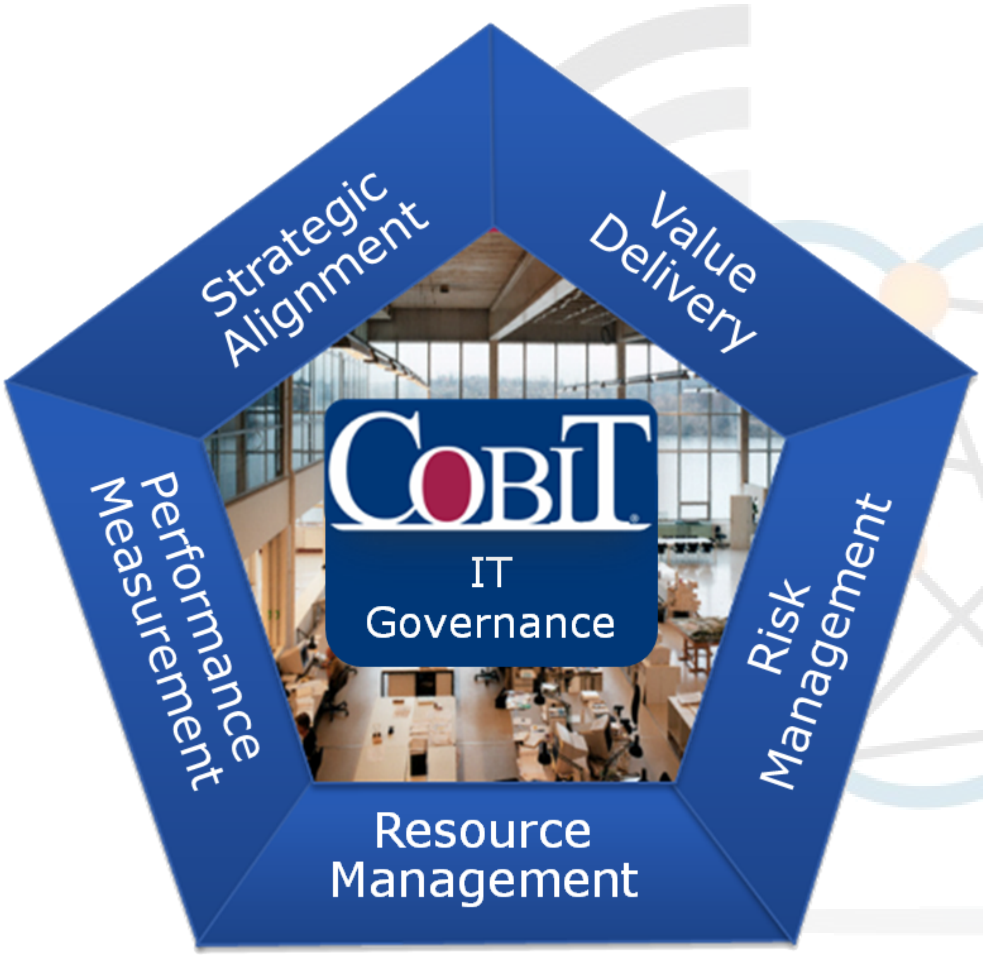


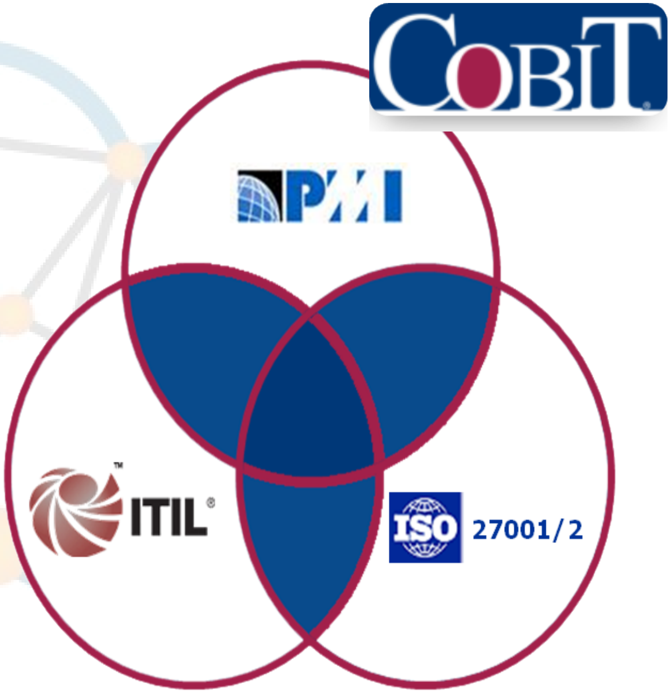
Cryptography

- Asymmetric key cryptography
  - Bob and Alice



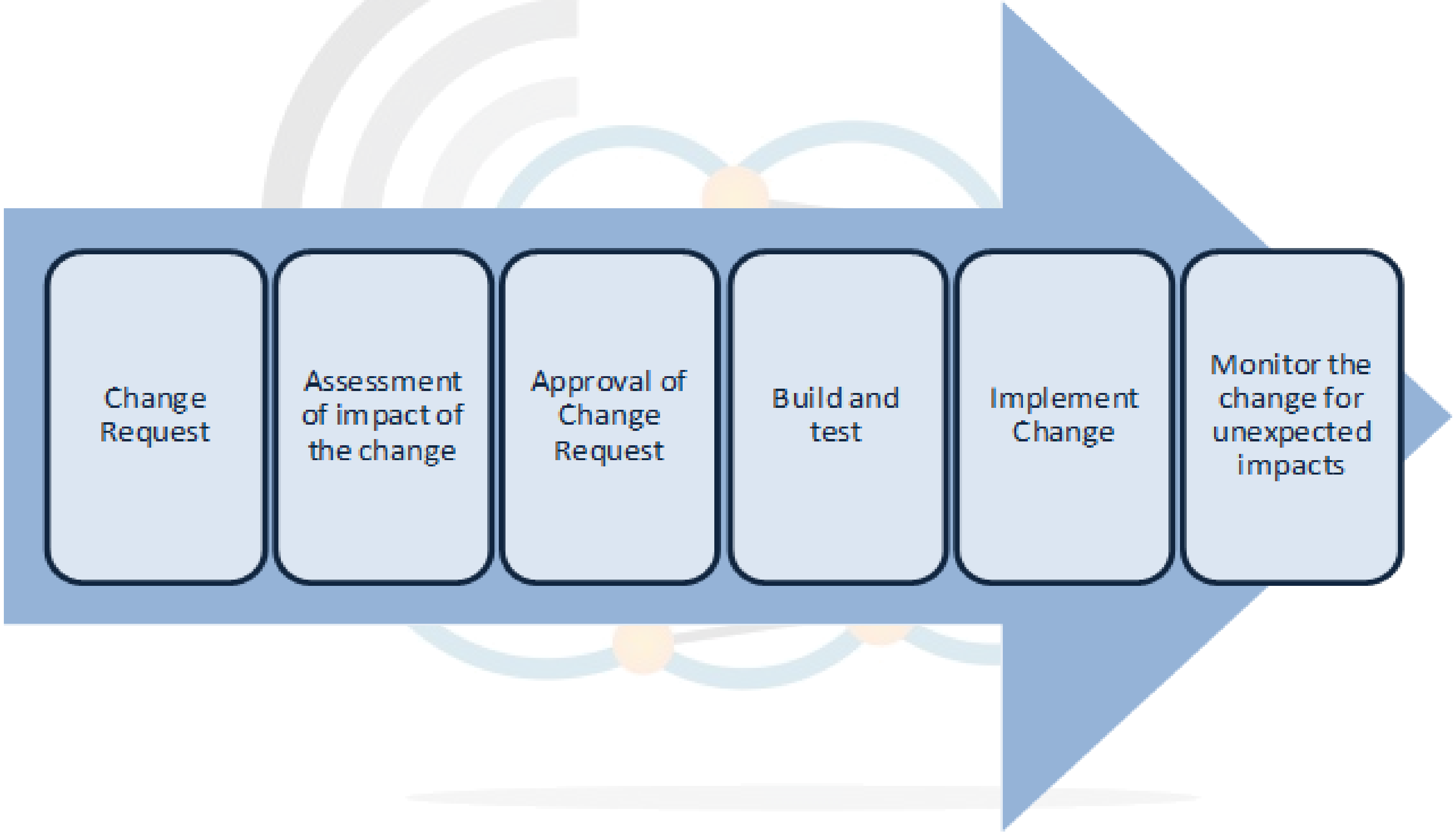
CobiT IT Governance





Change Management

- Change Management is the process of managing change.


Change Request
Assessment of impact of the change
Approval of Change Request
Build and test
Implement Change
Monitor the change for unexpected impacts

Data Classification

- Data Classification
  - Assign a level of sensitivity to data as it is being created, amended, enhanced, stored, or transmitted

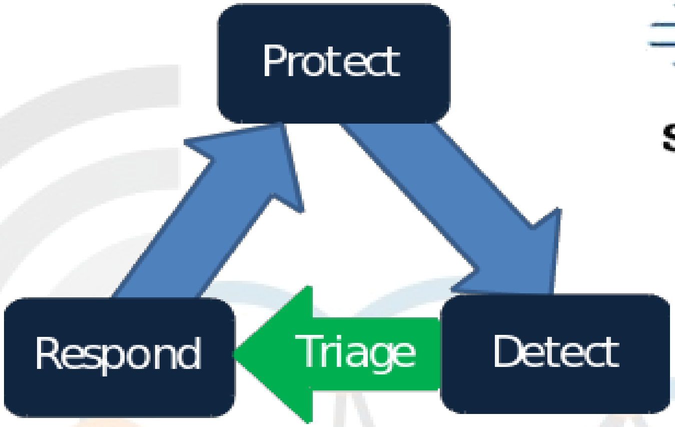
- Military
  - Top Secret
  - Secret
  - Confidential
  - Restricted
  - Unclassified

- Commercial
  - Confidential
  - Private
  - Sensitive
  - Public

Incident Management

NIST

Software Engineering Institute



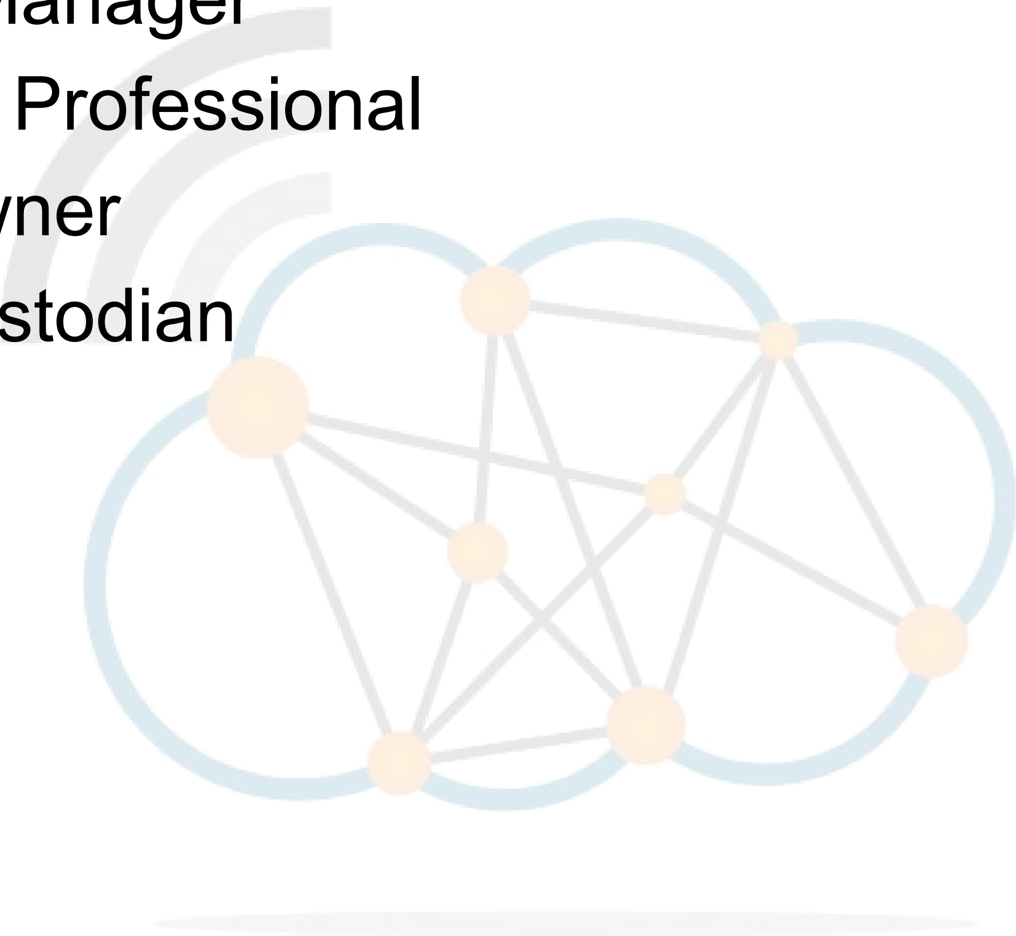
- **Proactive preparation**
  - The preparation of policies to deal with possible events and the implementation of a continuous cycle of auditing and improvement of these policies.
- **Reaction**
  - Measures carried out on the detection of an incident. How the incident was detected, what triage classification and prioritisation was carried out and how the response was conducted.

Hiring new staff

- Creating a Job Description
- Setting a classification for the job
- Screening candidates
- Hiring and Training the selected candidate
- Non Disclosure Agreements (NDA).
  -
- Separation of Duty (SoD)
  - The principle requires that the certifier of a transaction and the implementer be different entities.

Security roles

- Senior Manager
- Security Professional
- Data Owner
- Data Custodian
- User
- Auditor.



Data Protection & Privacy

- Data Protection and Privacy Bill, 2016
  - Principles of Data Protection
  - Data Collection and Processing
    - Consent, protection of privacy
  - Security of Data - breach notification to NITA-U
  - Rights of subjects
    - Access, prevent processing, etc..
  - Sanctions
    - Individuals: 4,800,000 Ugx and/or 10 years prison.
    - Corporations: All individuals involved.

Digital Evidence

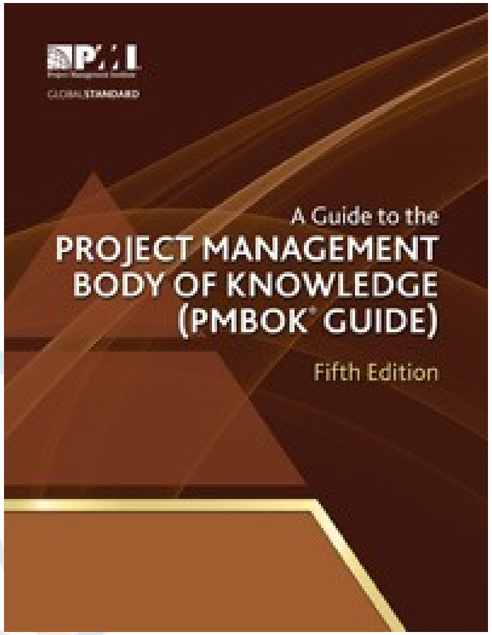
- Preservation
  - Original state
  - Forensic duplicate.
- Chain of Custody
  - Who
  - What
  - When
  - Where
  - How.

- Process of investigation
- Identify:
  - Suspects
  - Systems
  - Witnesses
  - Investigative team
  - Search warrants.
- File ownership
- Modification records.
- Means, Opportunity & Motives (MOM)
- Modus Operandi (MO).

Project Management

- PMI
- PRINCE2

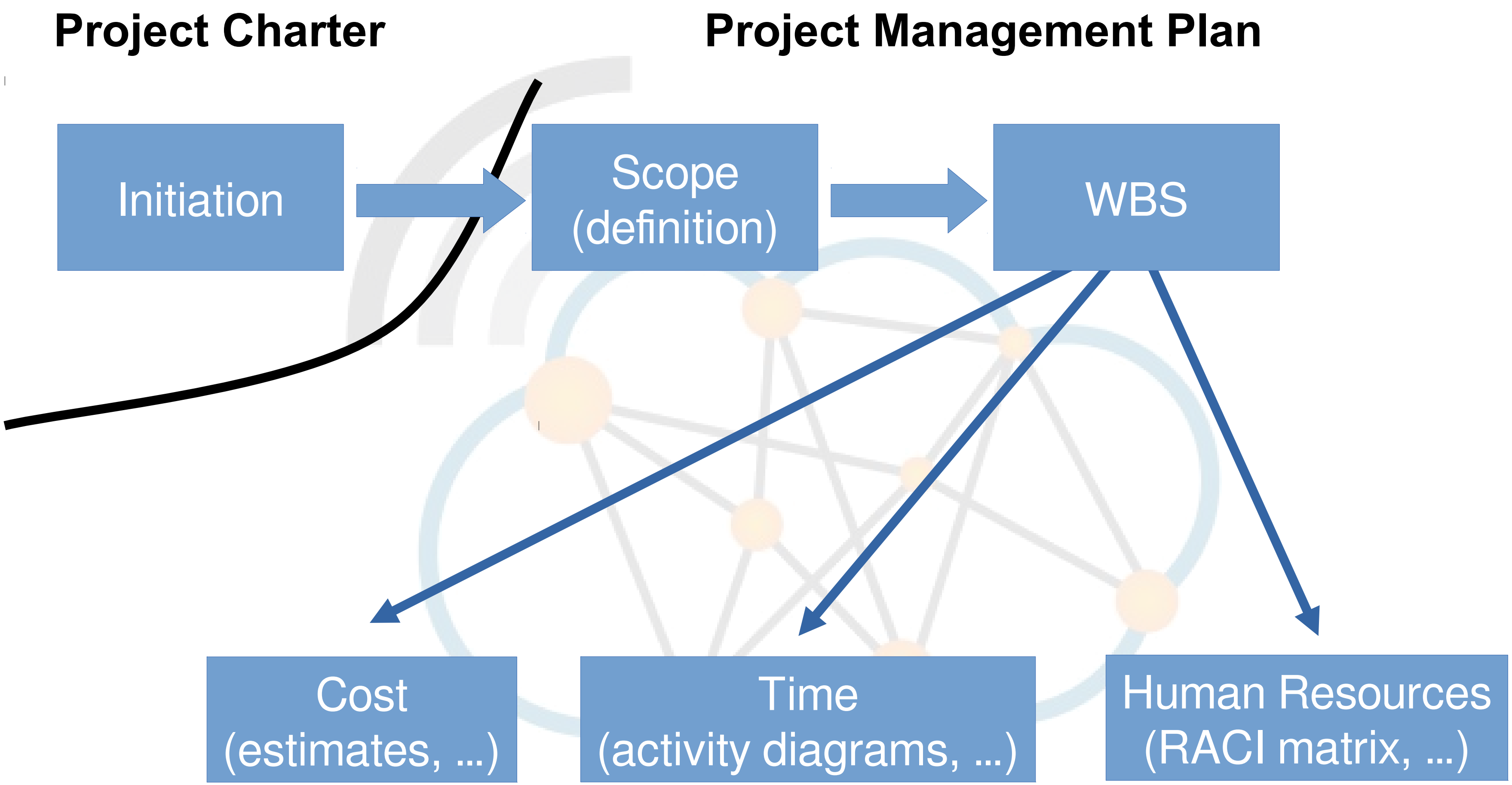
- Project Management Office
  - Project repository
  - Project Coach Model
  - Enterprise PMO
  -
- Project Management terms
  - Forward pass calculation
  - Backward pass calculation
  - Critical path



PMI®
Project Management Institute

PRINCE2®

Project Management Processes



Project Charter

Project Management Plan

Initiation

Scope (definition)

WBS

Cost (estimates, …)

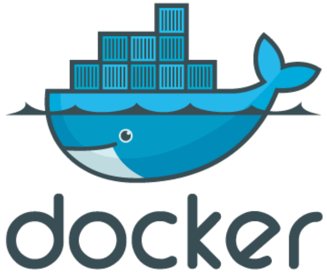
Time (activity diagrams, …)

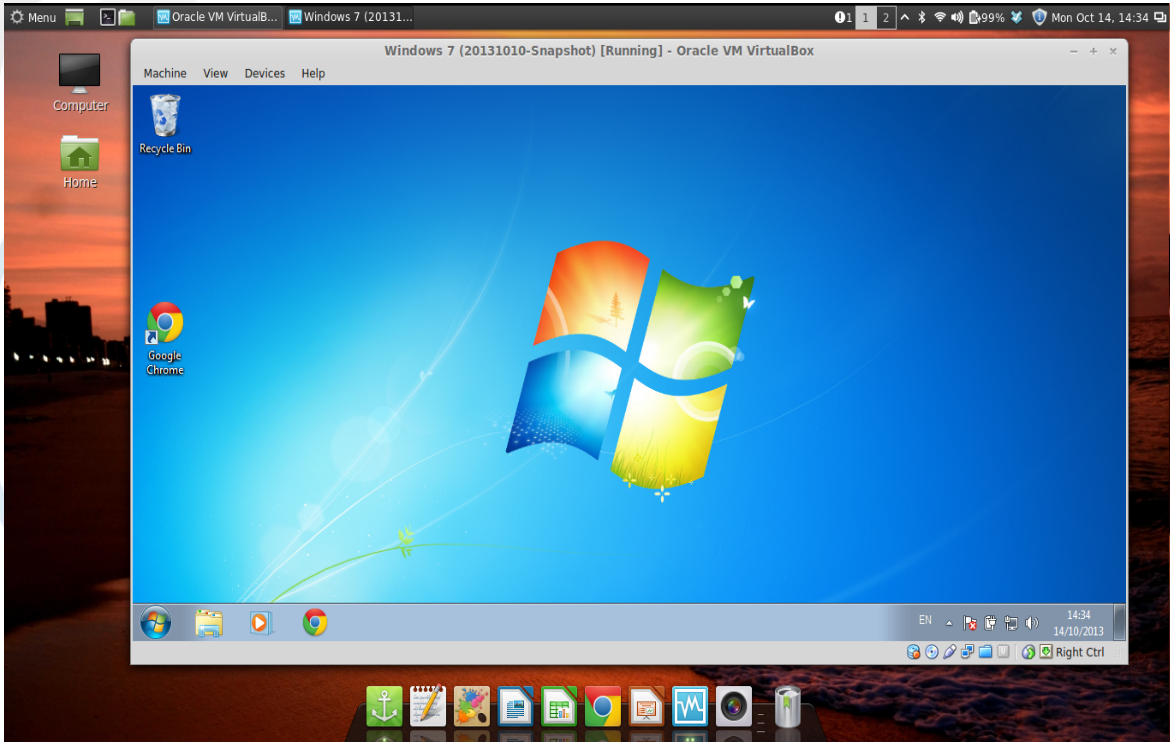
Human Resources (RACI matrix, …)

- Also to consider: Quality, Risk, Communication, Procurement, Integration.

Virtualisation

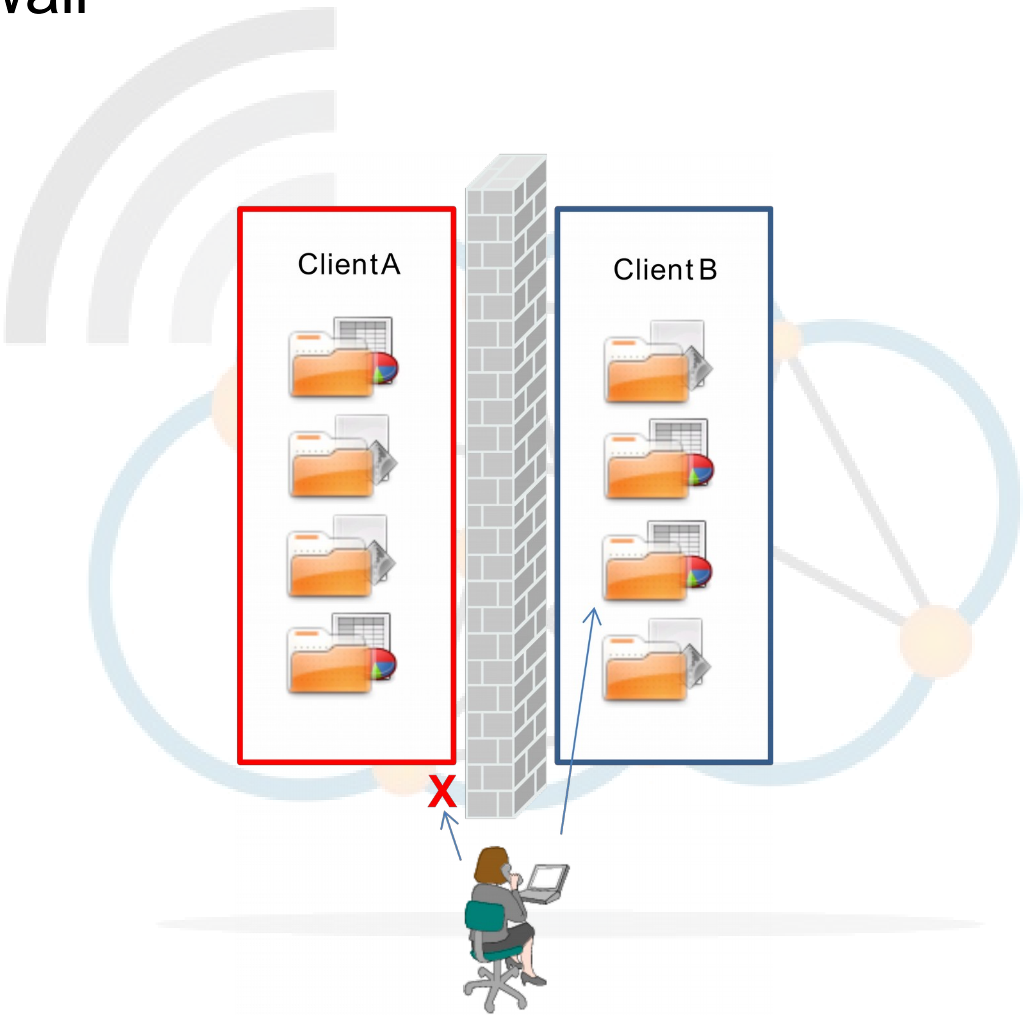
- Type 1 – baremetal
- Type 2





Brewer and Nash model

- Chinese wall



Evaluation Criteria

- Common Criteria (ISO/IEC 15408)

Common Criteria for Information Technology Security Evaluation

Center for Internet Security

- **Offence informs defence**
  - Knowledge of actual attacks inform defences.
  - Include only those controls that can be shown to stop known real-world attacks.
- **Prioritisation**
  - Invest first in Controls that will provide the greatest risk reduction.
- **Metrics**
  - Establish common metrics to provide a shared language for everyone.
- **Continuous diagnostics and mitigation**
  - Carry out continuous measurement.
- **Automation**
  - Automate defences.

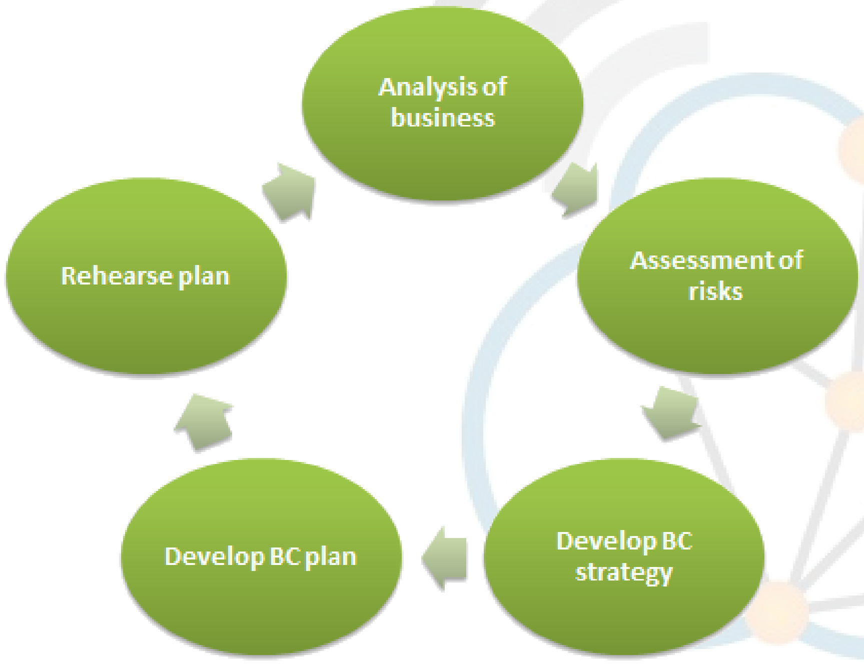
CIS
Critical
Security
Controls

The first 5 CSCs

- **Foundational Cyber Hygiene**
  - 80% of attacks.
  - **CSC 1 : Inventory of Authorised and Unauthorised Devices**
    - Define a baseline of what must be defended.
    - Prevent unauthorised devices from joining a network.
  - **CSC 2 : Inventory of Authorised and Unauthorised Software**
    - Only authorised software is allowed to execute on an organisation's information systems.
  - **CSC 3 : Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**
    - Securely configure their systems at scale.
      - Unix/Linux systems Ansible, Puppet or Chef are available
      - Microsoft there is the Active Directory Group Policy Objects.
  - **CSC 4 : Continuous Vulnerability Assessment and Remediation**
    - Patch management system
    - Vulnerability management system.
  - **CSC 5 : Controlled Use of Administrative Privileges**
    - Workforce members have only the system rights, privileges and permissions that they need in order to do their job.

Business Continuity Planning (BCP)

- BS 25999 - Business Continuity Management (BCM)



- Accept the risk
- Accept the risk but partner
- Reduce the risk
- Reduce the risk but partner.

Business Impact Assessment (BIA)

- For each urgent function, two values are then assigned:
  - ***Recovery Point Objective (RPO)*** - the acceptable latency of data that will be recovered
  - ***Recovery Time Objective (RTO)*** - the acceptable amount of time to restore the function
- The RPO must ensure that the ***Maximum Tolerable Data Loss (MTDL)*** for each activity is not exceeded. The RTO must ensure that the ***Maximum Tolerable Period of Disruption (MTPD)*** for each activity is not exceeded.

Business Impact Assessment (BIA)

- Identify the key business processes and technology components that would suffer the greatest financial, operational, customer, and/or legal and regulatory loss in the event of a disaster.
- The BIA identifies all the critical resources, systems, facilities, records, etc., that are required for BC.
- For each entry in BIA identify the time it would take to recovery such resources.

Business Plan

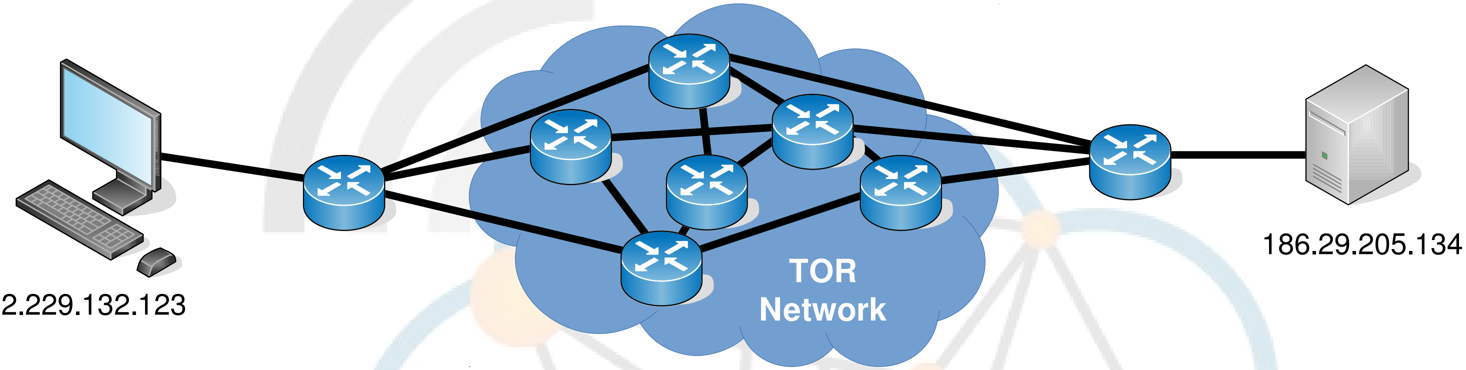
- Develop a Business Plan
- Business Impact Assessment (BIA)
  - Recovery Point Objective (RPO)
  - Recovery Time Objective (RTO)
  - Maximum Tolerable Data Loss (MTDL)
  - Maximum Tolerable Period of Disruption (MTPD).
- Rehearse Plan.

What steps are used to carry out pen test

- Planning and Preparation
- Information Gathering and Analysis
- Vulnerability Detection
- Penetration attempt
- Analysis and Reporting
- Cleaning up

Testing with Anonymity – The Onion Router

- The Onion Router (TOR)
- ProxyChains.



```
cedat:~$ proxychains nmap -Pn -sT -p 22,80 186.29.205.134
ProxyChains-3.1 (http://proxychains.sf.net)

Starting Nmap 6.40 ( http://nmap.org ) at 2015-11-04 22:07 EAT
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:80-<><>-OK
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:80-<><>-OK
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:22-<><>-OK
Nmap scan report for li489-237.members.linode.com (186.29.205.134)
Host is up (0.61s latency).
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

OWASP

- Open Web Application Security Project (OWASP) is an open community dedicated to enabling organisations to:
  - Conceive
  - Develop
  - Acquire
  - Operate
  - Maintain
- applications that can be trusted.

- All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security.

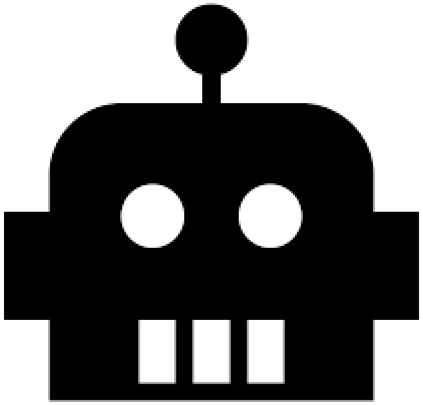
OWASP ZAP

- The OWASP ZAP is an integrated penetration testing tool for finding vulnerabilities in web applications.
- It can be used by developers and function test engineers to carry out penetration testing to identify and close vulnerabilities on their web developments.

Methods of Attack

OWASP
The Open Web Application Security Project

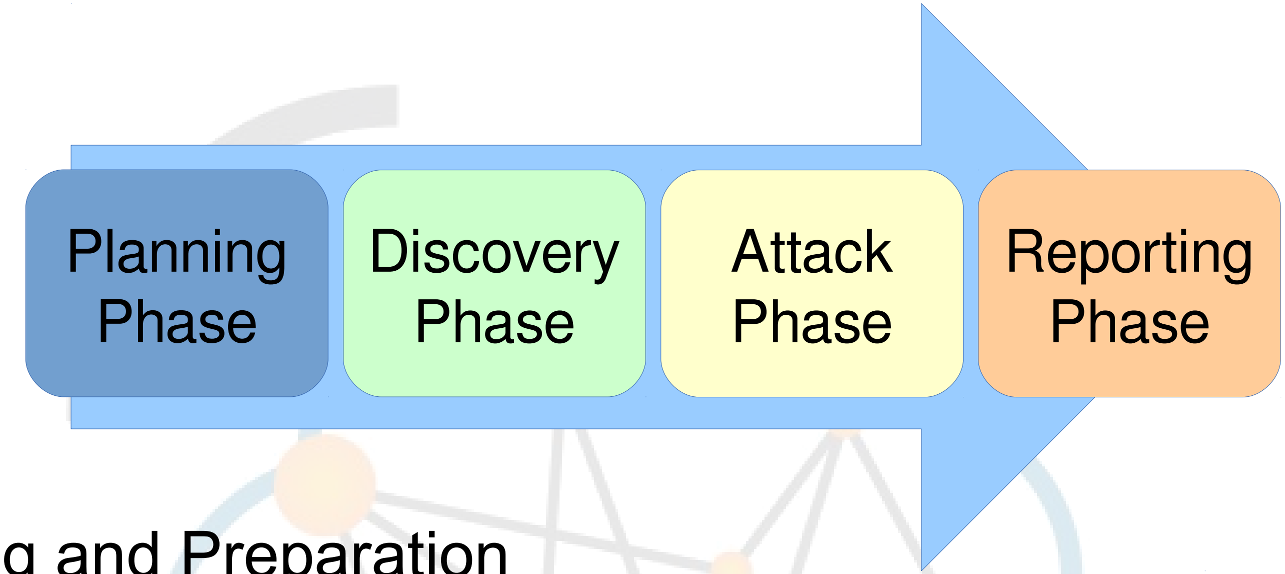
- Time Of Check To Time Of Use (TOCTTOU)
- Denial of Service (DoS)
- Smurf
- SYN Flood
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)



Monitoring – fingerprinting tool (p0f)

```
~$ sudo p0f -i eth0 -do /tmp/p0f-output.txt
<Tue Nov 7 08:41:17 2017> 109.126.43.68:49090
- UNKNOWN [S20:64:1:60:M1460,S,T,N,W7:.:?:?]
(up: 9054 hrs) -> 41.220.223.38:80 (link:
ethernet/modem)
```

What steps are used to carry out pen test



- Planning and Preparation
- Information Gathering and Analysis
- Vulnerability Detection
- Penetration attempt
- Analysis and Reporting
- Cleaning up

National Information Technology Authority Uganda

Uganda - Integration of National Databases project

Finally a tip

- Read the narrative carefully before the exam:

- Beidh and t-ádh agaibh ar an lá

(May luck be with you on the day)