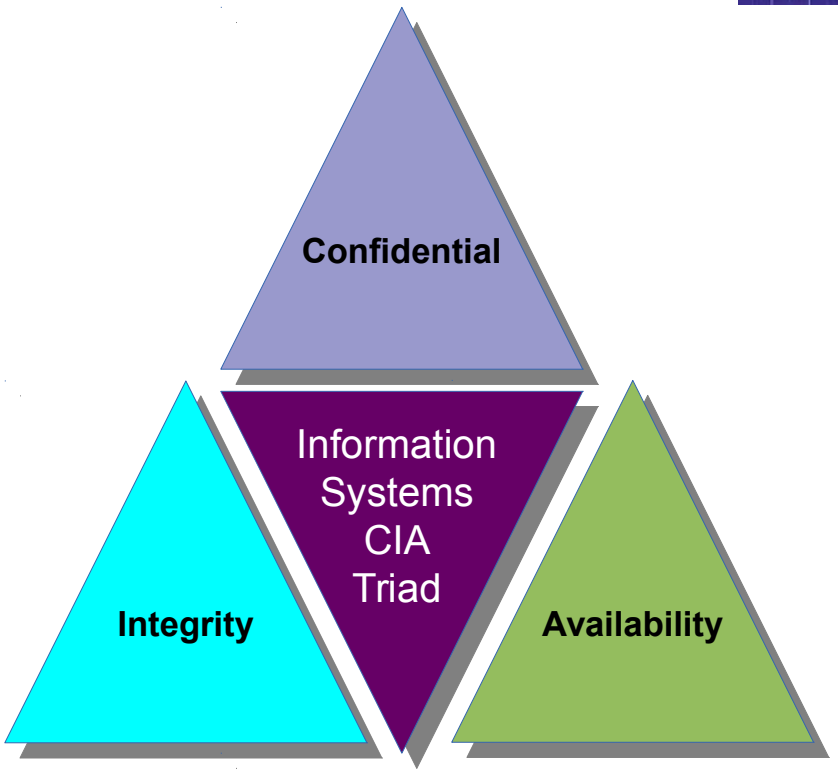
Operations Security

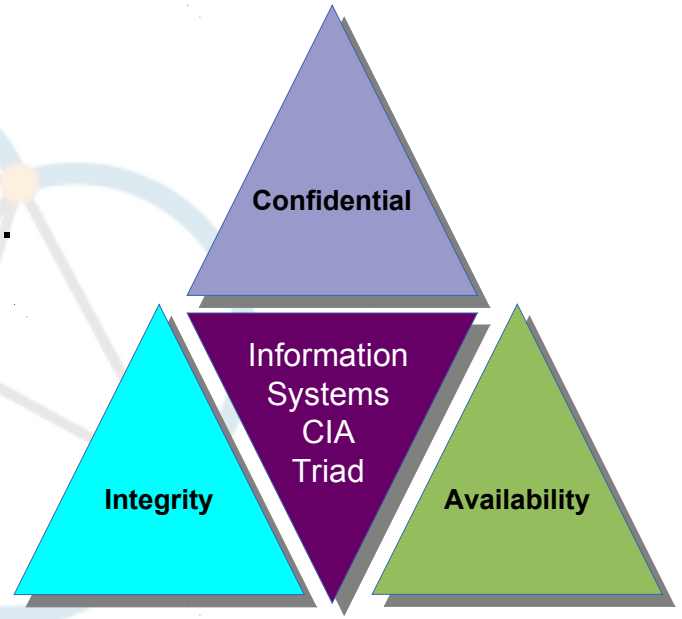


CISSP®
Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP
diarmuid@obriain.com

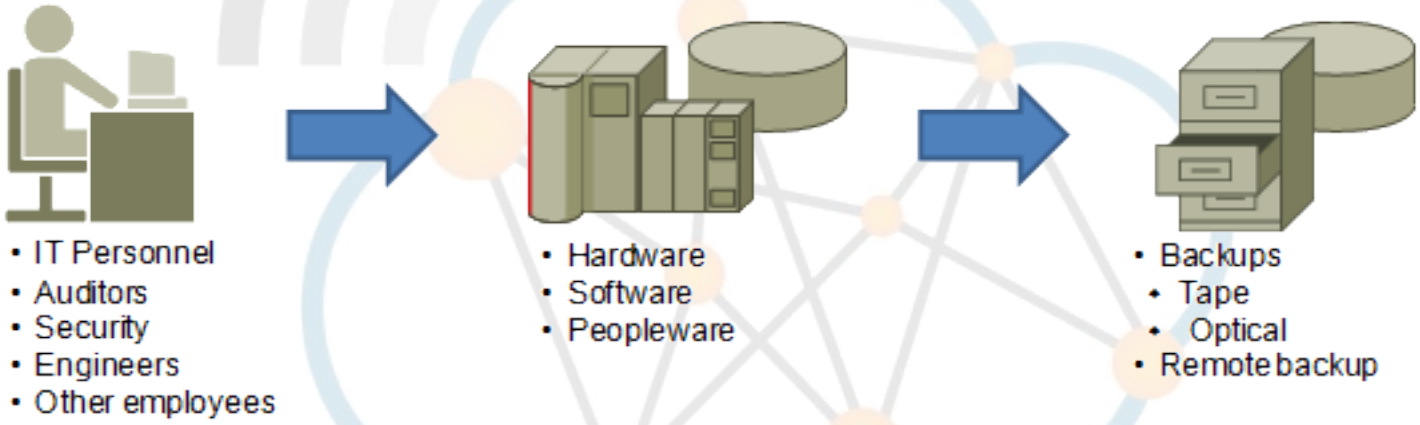
Information Systems Operations

- Information Systems Operations involves the confidentiality of integrity of information and the availability of systems.

- Information Systems Operations is about:
  - Identifying the resources to be protected.
  - Defining the privileges that must be restricted.
  - Determining the available control mechanisms.
  - Appreciating the potential for abuse of access.
  - Ensuring the appropriate use of controls.
  - Implementing good security practice.



Operations focus



- IT Personnel
- Auditors
- Security
- Engineers
- Other employees

- Hardware
- Software
- Peopleware

- Backups
  - Tape
  - Optical
- Remote backup

Access Control Categories

CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Access Control Categories

- Preventive
- Deterrent
- Detective
- Corrective
- Recovery
- Compensation
- Directive
- Administrative
- Logical or technical
- Physical

Resource Protection

CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Resource protection

- Physical protection of equipment.
- Media Management
  - Storage
    - Temperature and Humidity Controlled Environment.
    - Static Free Surroundings.
    - Fire Suppressant Systems.
    - Fire Protection.
  - Encryption.
  - Retrieval.
  - Disposal.
  - Marking.
- Records management.
- Fire.
- Property protection.
- Electrical Power.
- HVAC.
- Water.
- Communications.

Administrative Control

CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Administrative control

- Enforce company policies on behalf of management.
- Ops team must be trustworthy
  - Guardians of the network.
  - Log activities of Operations team.
  - Access on a strict ‘need to know’ basis.
- Separation of duties (SoD)
  - System Administrator.
  - Security Administrator.
  - Network Administrator.
  - Database Administrator.
  - E-mail Administrator.

Administrative control

- Job Rotation
  - Succession planning.
- Mandatory Vacations.
- Security Violations
  - Root cause.
  - Documented.
  - Process change where necessary.
- Disciplinary process
  - Harsh for security violations.
  - Termination.

Center for Internet Security®

Center for Internet Security (CIS)

Critical Security Controls (CSC)

CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Center for Internet Security (CIS)

- 2008 - collaboration between representatives from the U.S. government and private sector security research organisations.
- **CIS Critical Security Controls (CSC)**
  - Practical defences specifically targeted toward stopping cyber attacks
  - Technical in nature
  - Define specific, practical steps an organisation can take to stop the most common cyber threats from compromising their information systems.

"***Where should I start when I want to improve my cyber defences?***"

CIS tenets of an effective cyber defence system

- **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.

The first five 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.

Remaining CSCs

- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs.
- CSC 7: Email and Web Browser Protections.
- CSC 8: Malware Defences
- CSC 9: Limitation and Control of Network Ports, Protocols, and Services.
- CSC 10: Data Recovery Capability.
- CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches.
- CSC 12: Boundary Defence.
- CSC 13: Data Protection.
- CSC 14: Controlled Access Based on the Need to Know.
- CSC 15: Wireless Access Control.
- CSC 16: Account Monitoring and Control.
- CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps.
- CSC 18: Application Software Security.
- CSC 19: Incident Response and Management.
- CSC 20: Penetration Tests and Red Team Exercises.

Information Systems Operations Functions

CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Threat Awareness

- Media Libraries.
- Errors and Omissions.
- Fraud and Theft.
- Employee Sabotage.
- Loss of Physical Support.
- Industrial Espionage.
- Loss of infrastructure support.
- Hackers.
- Malicious code
  - Worms.
  - Viruses.
  - Trojan horses.

Protection of Information

- Backup of Critical Information regularly.
- Perform off-site backups.
- Redundancy
  - High Availability (HA).
  - RAID.
- System trusted recovery.

Fault tolerant systems

- No single point of failure.
- No single point of repair.
- Fault isolation to the failing component.
- Fault containment to prevent propagation of the failure.
- Availability of reversion modes.

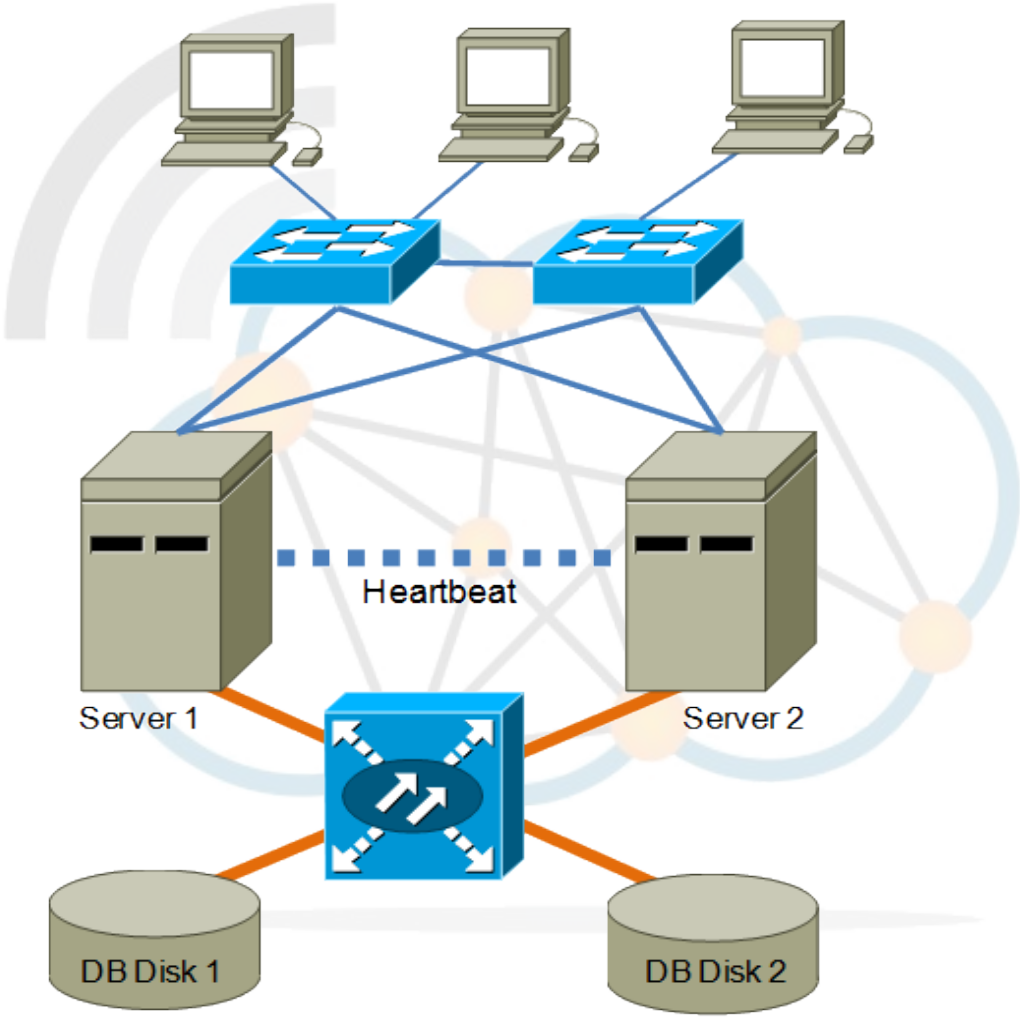
Fault tolerant systems

- **Hot Standby**
  - The primary and backup systems run simultaneously.
  - The data is mirrored to the secondary server in real time.
- **Warm Standby**
  - The backup system runs in the background of the primary system.
  - Data is mirrored to the secondary server at regular intervals.
- **Cold Standby**
  - The backup system is only called upon when the primary system fails.
  - The system on cold standby receives scheduled data backups, but less frequently than a warm standby.
  - Cold standby systems are used for non-critical applications or in cases where data is changed infrequently.

Fault tolerant systems

- **Replication**
  - Providing multiple identical instances of the same system or subsystem, directing tasks or requests to all of them in parallel, and choosing the correct result on the basis of a quorum.
- **Redundancy**
  - Providing multiple identical instances of the same system and switching to one of the remaining instances in case of a failure (failover).
- **Diversity**
  - Providing multiple different implementations of the same specification, and using them like replicated systems to cope with errors in a specific implementation.

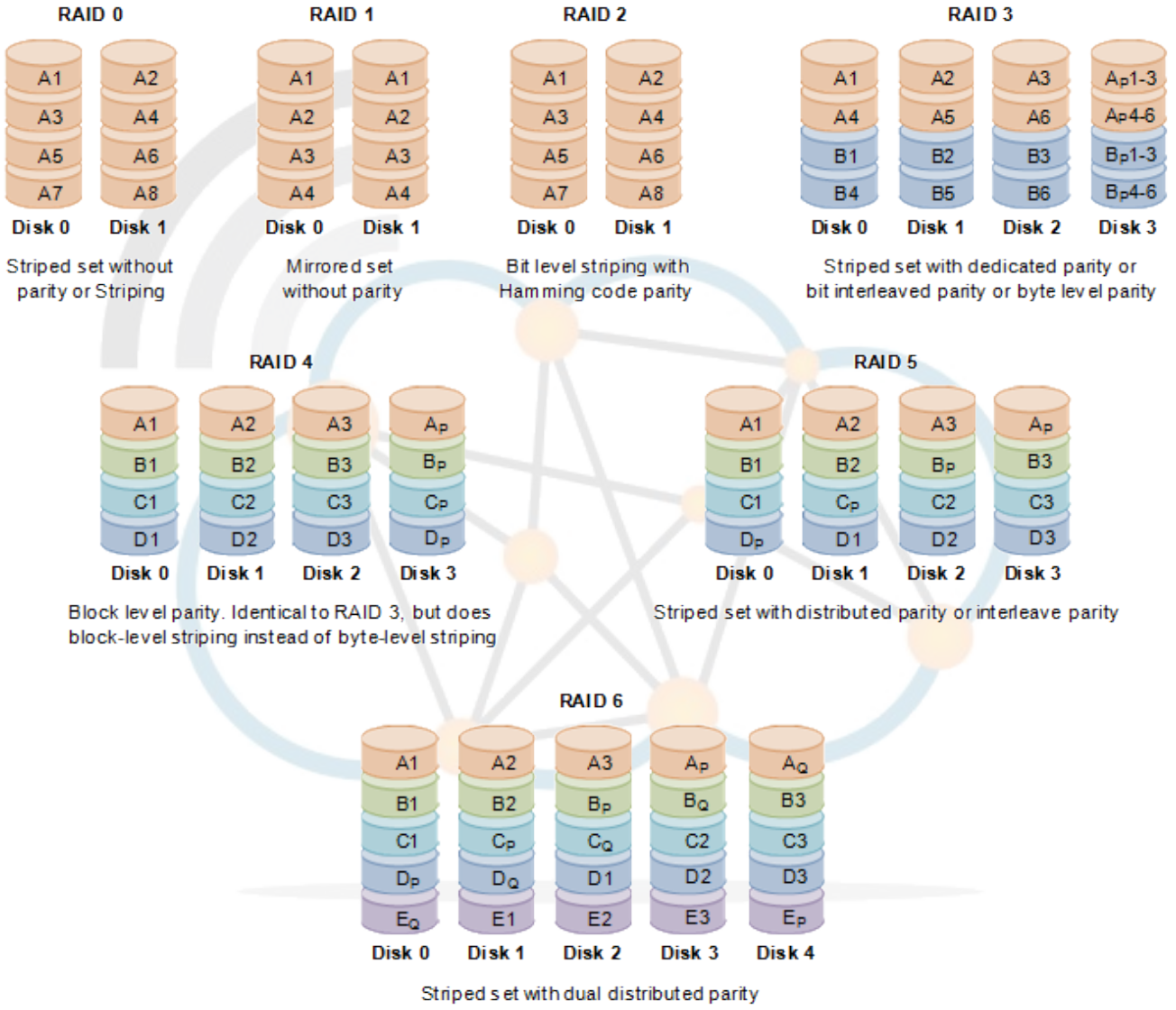
High Availability Clusters



Redundant Array of Inexpensive/Independent Disks RAID

- RAID achieves high levels of storage reliability from low-cost and less reliable PC-class disk-drive components.
- There are various combinations giving different trade-offs of protection against data loss, capacity, and speed.
- RAID levels 0, 1, and 5 are the most commonly found, and cover most requirements.
- **Striping**
  - Distributes data across multiple disks.
  - Improves speed, one disk fails data is lost.
- **Mirroring**
  - Mirrors data on multiple disks.
  - Identical data on at least 2 disks.

RAID


RAID 0
A1
A3
A5
A7
A2
A4
A6
A8
Disk 0
Disk 1
Striped set without parity or Striping
RAID 1
A1
A2
A3
A4
A1
A2
A3
A4
Disk 0
Disk 1
Mirrored set without parity
RAID 2
A1
A3
A5
A7
A2
A4
A6
A8
Disk 0
Disk 1
Bit level striping with Hamming code parity
RAID 3
A1
A4
B1
B4
A2
A5
B2
B5
A3
A6
B3
B6
Ap1-3
Ap4-6
Bp1-3
Bp4-6
Disk 0
Disk 1
Disk 2
Disk 3
Striped set with dedicated parity or bit interleaved parity or byte level parity
RAID 4
A1
B1
C1
D1
A2
B2
C2
D2
A3
B3
C3
D3
Ap
Bp
Cp
Dp
Disk 0
Disk 1
Disk 2
Disk 3
Block level parity. Identical to RAID 3, but does block-level striping instead of byte-level striping
RAID 5
A1
B1
C1
Dp
A2
B2
Cp
D1
A3
Bp
C2
D2
Ap
B3
C3
D3
Disk 0
Disk 1
Disk 2
Disk 3
Striped set with distributed parity or interleave parity
RAID 6
A1
B1
C1
Dp
Eq
A2
B2
Cp
Dq
E1
A3
Bp
Cq
D1
E2
Ap
Bq
C2
D2
E3
Aq
B3
C3
D3
Ep
Disk 0
Disk 1
Disk 2
Disk 3
Disk 4
Striped set with dual distributed parity

System recovery

- **System Cold Start**
  - A normal system start not possible due to unexpected failures.
  - The Administrator will need to intervene to bring the system to a normal state.
  - Example
    - Reboot system to single user mode.
    - Recover all active file systems at the time of failure.
    - Restore missing or damaged files from backups.
    - Recover security labels to missing files.
    - Check security critical files.
    - Allow users access to the system.

System recovery

- **Emergency System Restart**
  - This is typical of when the system fails and brings itself to a maintenance mode to perform file recovery and restarts with none of the user process that existed at the time of the failure restored.

- **System Reboot**
  - This is carried out after the administrator has noticed a failure and shutdown the system in a controlled manner.

Change and Control Management

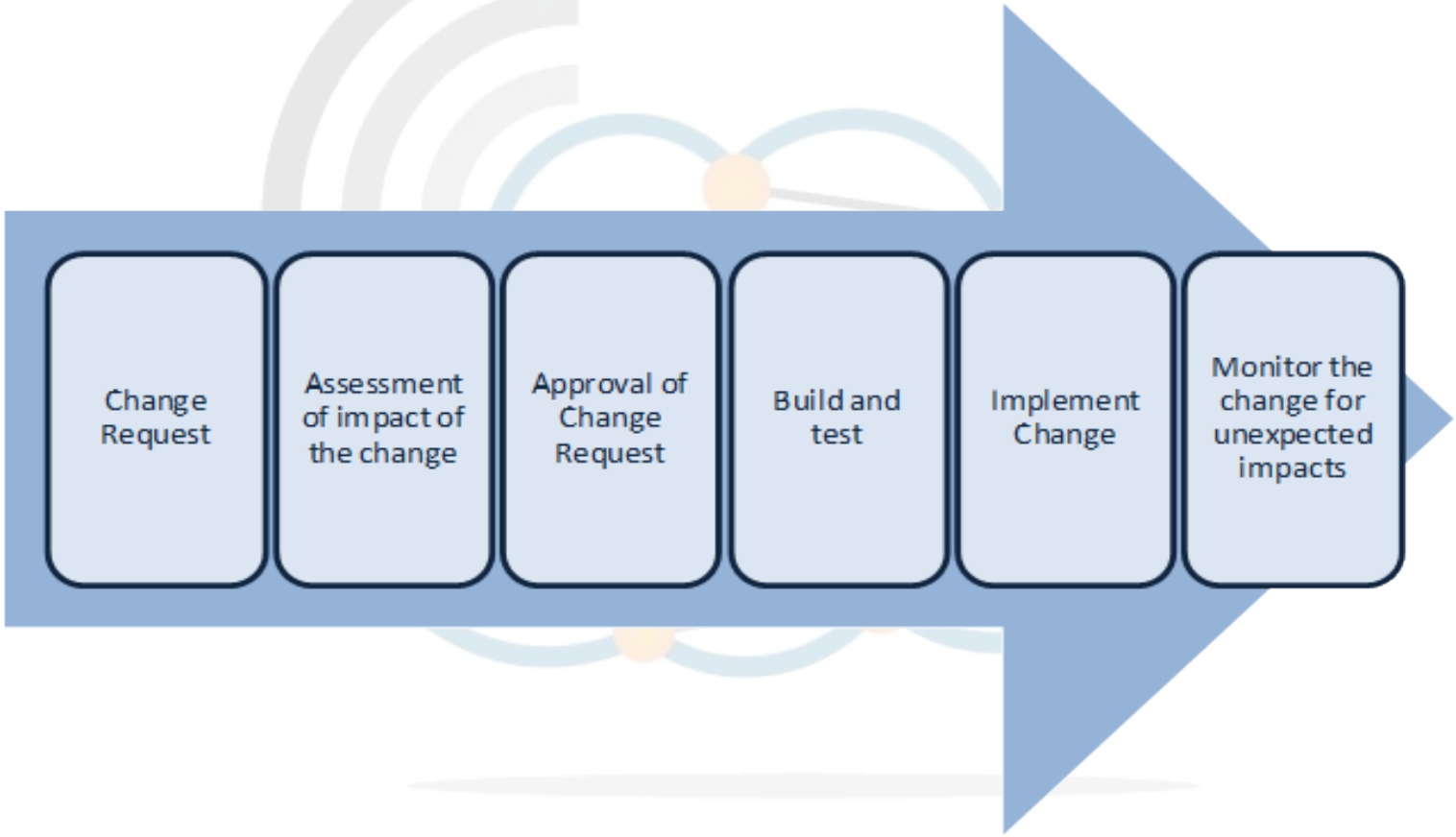
CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Change Management

- Change Management is the process of managing change.

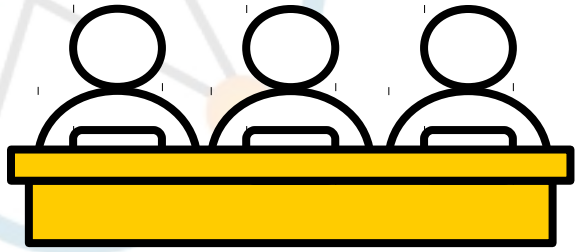


Change Control Procedures

- Record Change Request.
- Assessment of the impact of the change.
- Approval of the Change Request.
- Build and test.
- Implement Change.
- Monitor.

Group Exercise

- Consider a company who has built an online presence consisting of a redundant website, with on-line shopping facilities. They have dual site redundancy.
- Carry out in groups a plan for the system, consider:
  - Location of server(s)
  - Contracts with site owner(s).
  - Access Agreements.
  - Access Control.
  - High Availability.
  - Security.
  - Employee roles.
  - Operations policies.
  - Change Control Mechanisms.



Thank you