Topic 1 Operations, Business Continuity & Disaster Recovery

Dr Diarmuid Ó Briain

22 Jan 2025

setu.ie
INSPIRING FUTURES
Version: 1.1

Learning objectives

By the end of this topic, you will be able to:

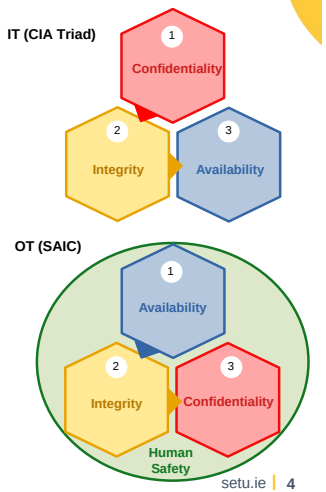
- Understand the principles of managing and protecting information systems operations.
- Apply effective access control strategies to protect information systems assets.
- Implement comprehensive resource protection measures to safeguard information systems.
- Develop and execute effective business continuity plans to mitigate disruptions.

Operations Security

Information Systems Operations

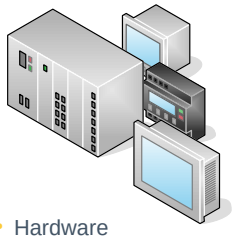
- Information Systems Operations involves the confidentiality of integrity of information and the availability of systems.

- 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.

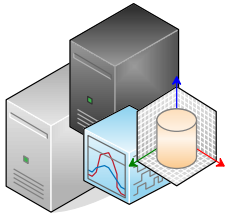


Operations focus

- Operations Personnel
- IT Personnel
- Auditors
- Security
- Engineers
- Other Employees



- Hardware
- Software
- Peopleware



- Backups
  - Tape
  - Optical
- Remote Backups

Access Control Categories

Access Control Categories

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

Resource Protection

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

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.

CIS

Center for Internet Security

SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

CIS Controls

Center for Internet Security (CIS)

- 2008 - collaboration between representatives from the U.S. government and private sector security research organisations.
- Current version 8 – Released October 2022
- Prioritised set of safeguards to mitigate the most prevalent cyber-attacks against systems and networks.
- They are considered the gold standard for cybersecurity best practices and are widely used by organisations of all sizes to improve their security posture.

CIS Controls focus

- Focus on activity-based controls
- Reduction in the number of controls
- Emphasis on hybrid and cloud environments

CIS Controls Design Principles

- **Offence Informs Defence**
- **Focus**
- **Feasible**
- **Measurable**
- **Align**

Implementation Groups

- **IG1** - Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks.
- **IG2** (Includes IG1) - An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission.
- **IG3** (Includes IG1 and IG2) - An IG3 enterprise employs security experts that specialise in the different facets of cybersecurity. IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight.

The CSCs

- CSC 1 - Inventory and Control of Enterprise Assets
- CSC 2 - Inventory and Control of Software Assets
- CSC 3 – Data Protection
- CSC 4 – Secure Configuration of Enterprise Assets and Software
- CSC 5 – Account Management
- CSC 6 – Access Control Management
- CSC 7 – Continuous Vulnerability Management
- CSC 8 – Audit Log Management
- CSC 9 – Email and Web Browser Protections

The CSCs

- CSC 10 – Malware Defences
- CSC 11 – Data Recovery
- CSC 12 – Network Infrastructure Management
- CSC 13 – Network Monitoring and Defence
- CSC 14 – Security Awareness and Skills Training
- CSC 15 – Service Provider Management
- CSC 16 – Application Software Security
- CSC 17 – Incident Response Management
- CSC 18 – Penetration Testing

CSC Safeguards example

- CSC 1 - Inventory and Control of Enterprise Assets
  - Safeguard 1.1 - Establish and Maintain Detailed Enterprise Asset Inventory
    - Security function: Identify IGs 1, 2 and 3.
  - Safeguard 1.2 - Address Unauthorised Assets
    - Security function: Respond IGs 1, 2 and 3.
  - Safeguard 1.3 - Utilise an Active Discovery Tool
    - Security function: Detect IGs 2 and 3.
  - Safeguard 1.4 - Use DHCP Logging to Update Enterprise Asset Inventory
    - Security function: Identify IGs 2 and 3.
  - Safeguard 1.5 - Use a Passive Asset Discovery Tool
    - Security function: Detect IG 3.

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Information Systems Operations Functions

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.

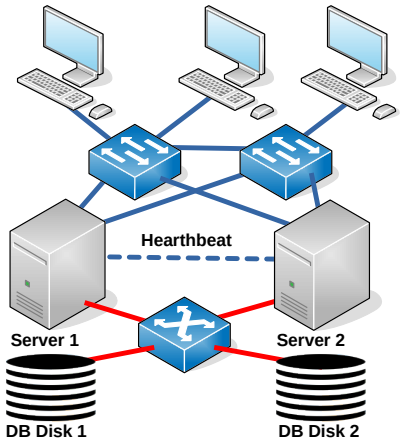
Fault tolerant systems

- **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.

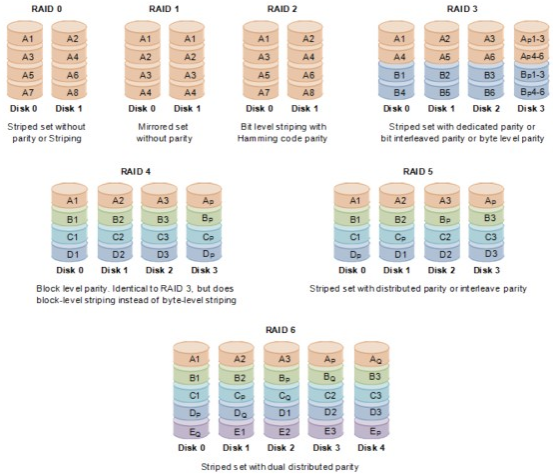
High Availability Clusters



Redundant Array of Inexpensive 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



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

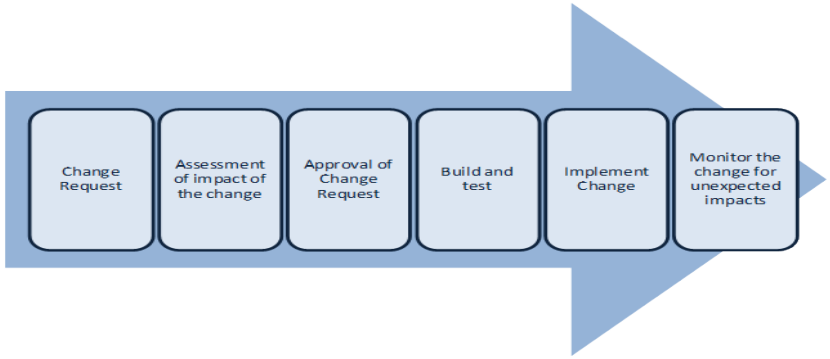
- **Emergency System Restart**
  - This is typical of when the system fails and brings itself to a maintenance mode to perform file recovery and restarts with none of the user process that existed at the time of the failure restored.
- **System Reboot**
  - This is carried out after the administrator has noticed a failure and shutdown the system in a controlled manner.

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Change and Control Management

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, for Just In Time (JIT) manufacturing, consisting of a redundant website, with on-line ordering 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.

15

SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

Business Continuity Planning

BCP Standards

- **ISO 22301:2019 - Business Continuity Management Systems**
  - Requirements for an organisation's Business Continuity Management System (BCMS)
  - Systematic approach to ensuring that the organisation can continue to operate critical business functions in the event of a disruptive event.
- **ISO 27031:2011 - ICT readiness for Business Continuity**
  - Guidance on how to implement an ICT readiness capability for business continuity.
- **NIST SP 800-82r3**
  - Outlines the steps to develop recovery and restoration capability to recover from cybersecurity incidents and to restore the assets and services that were impaired by the cybersecurity incident to a pre-cyber- incident state.

NIST SP 800-82r3 Recovery and Restoration

- Define recovery objectives when recovering from disruptions
- Develop a site Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) to prepare the OT organisation to respond appropriately to significant disruptions in their operations due to the cybersecurity incident.
- Establish backup systems and processes to support recovery to a stable state.
- Establish processes for restoring relevant OT systems from backups in a timely manner.
- Establish recovery processes and procedures that will be executed to restore assets and services affected by cybersecurity incidents.
- Establish communication plans to coordinate restoration activities and to manage public relations.
- Establish a task for lessons learned as part of the recovery process.
- Test these plans at reasonable intervals that are appropriate for the organisation.

Business Continuity Planning (BCP)

Feature	ISO 22301	ISO 27031	NIST SP 800-82r3
Scope	Overall business continuity, including OT	ICT readiness for business continuity, specifically focusing on IT systems and infrastructure supporting OT	OT-specific business continuity, addressing the unique security and operational challenges of OT environments
Focus	Maintaining business operations, including OT	Recovering ICT services and infrastructure, including those supporting OT	Protecting critical OT assets, minimising downtime, preventing data loss, and preserving operational continuity
Requirements	More detailed and prescriptive, with specific guidelines for developing and implementing BCP procedures	More flexible and adaptable, allowing organisations to tailor BCP strategies to their specific IT environment	OT-specific and prescriptive, providing guidance on addressing cyber security threats and disruptions specific to OT systems
OT Considerations	Provides general guidelines for addressing OT security in the context of overall business continuity	Limited OT-specific guidance, focusing on ICT security measures for OT systems	Comprehensive OT security guidance, addressing risk assessment, control implementation, incident response, and recovery strategies

Business Continuity Lifecycle

Business Continuity Strategy

- BC Strategies will normally be determined by available budget, either:
  - Accept the risk.
  - Accept the risk but get a BC partner who can help in the event of an incident.
  - Reduce the risk.
  - Reduce the risk but get a BC partner who can help in the event of an incident.
  - Reduce the risk adequately that a BC partner is not necessary.

Business Plan

- **Develop a Business Plan**
  - Now that risks have been identified and a strategy to deal with them decided a full business plan will be needed. Such a plan should be simple because employees will need to act quickly and decisively after an incident.
- **Rehearse Plan**
  - There is a military maxim that applies at this stage "*Train hard, fight easy*". The plan must be rehearsed so that employees will know exactly what to do in the event of an incident.

Business Continuity Planning Process

Project scope and planning

- Structured analysis of the whole business for crisis management.
- Appointment of a BCP team with SMT approval. The team should consist of:
  - Representation from each department with responsibility for the company core systems
  - Representation from support departments
  - IT personnel with technical expertise in the core systems
  - Information Security officer
  - Legal representation with knowledge of the contractual requirements
  - SMT representative.
- Identification of all resources available to the team for BCP.
- Understanding of the regulatory and legal situation that governs the organisation's response to an major event requiring a BC response.

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 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.

Risk Analysis

- Recovery requirements are now defined, so an identification and documentation of potential risks should be undertaken.
- Identify the risks which gives the opportunity to review each and define a specific set of work instructions.
  - Terrorism
  - Cyber attack
  - Sabotage
  - Disease
  - Fire
  - Flood
  - Utility outage
  - …..

Assessment of Likelihood

- Now that we have identified risks what is the likelihood of these occurring?
- For each identified risk produce an ***Annualised Rate of Occurrence (ARO)***.
  - How often is it likely that this event will occur in any year?

Assessment of Impact

- Should an identified risk actually occur what is the likely impact of the event on the business?
- Determine the ***Exposure Factor (EF)*** to the business as a percentage of the ***Assets Value (AV)*** and from these figures calculate the ***Single Loss Expectancy (SLE)***:
  - SLE = AV × EF
- From the earlier ARO figure, it is a simple matter to calculate the **Annualised Loss Expectancy (ALE)**:
  - ALE = SLE × ARO

Prioritisation of Resources

- Taking all the risks analysed sort them in a descending list ordered by the ALE of each risk.

Continuity Planning

- **Strategic**: For each risk, is a BCP absolutely necessary?
- **Activity**:
  - People, workforce, skills and knowledge
  - Premises
    - Alternative Sites
  - Infrastructure
    - IT Backbone
    - Servers
    - Workstations
  - Information
    - Backup off site
  - Stakeholders partners and contractors
    - Alternative partners and contractors

Documentation

- Continuity Planning Goals
  - “To ensure the continuation of the business in the event of an emergency”
- Senior Executive Statement
  - Statement from the C-level management to indicate the importance of the BCP.
- Timetable
- Priority List
- Risk Assessment - BIA
- Records
- 'Action-on’ Emergency Incident
- Change process

Exercise #1.1

Group Exercise:
Business Continuity and Disaster Recovery

- As the CISO for a specialised Pharmaceutical company in Ireland. The company manufactures a combined calcium and vitamin medications for customers who underwent stomach surgery. The company specialises in direct sales and as such your company holds sensitive customer data that should not leave Ireland and strictly cannot leave the EU.
- The company currently operates a pair of cloud hypervisor servers in a data centre in Limerick and a private data centre in Carlow. These servers offer HA Hipervisor to the virtual servers.
  - Develop a BIA for 3 key business processes and technologies.
  - Carry out a risk assessment and list 5 key risks.
  - Order the risks.
  - Describe the mechanism used to order the risks.
  - Assuming the only risks are the 5 identified and develop a short BCP for them.
  - Suggest a test regime for the BCP.

30

Learning objectives

- Understand the principles of managing and protecting information systems operations ✓
- Apply effective access control strategies to protect information systems assets ✓
- Implement comprehensive resource protection measures to safeguard information systems ✓
- Develop and execute effective business continuity plans to mitigate disruptions ✓

Dr Diarmuid Ó Briain
Innealtóir Cairte agus
Léachtóir Sinsearach

D +353 59 917 5426 | E diarmuid.obriain@setu.ie | **setu.ie**
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire

Thank you

engcore
advancing technology