

ISMS Architecture, Regulatory Audits & Forensic Readiness

Dr Diarmuid Ó Briain

21 Oct 2026

Licence



This work is licenced under a Creative Commons
Attribution-ShareAlike 4.0 International Licence.
Full Licence: <http://creativecommons.org/licenses/by-sa/4.0>

Learning objectives

- At the end of this topic you will be able to:
 - Analyse the Core Architecture of ISO/IEC 27001 and the structural relationship between the Annex SL and the operational security controls of Annex A.
 - Describe the end-to-end strategy for transitioning an ISMS from initial project planning to operational readiness, culminating in internal reviews and formal Stage 1 and Stage 2 external certification audits.
 - Differentiate between the foundational management auditing principles of ISO 19011 and the specialised cybersecurity requirements of ISO/IEC 27007 to evaluate how compliance evidence is gathered and verified.
 - Explain the intersection of cybersecurity with liability law, CNI regulations, and the foundational requirements for preserving a strict chain of custody during digital forensic evidence collection.

The
Architecture
of
ISO
27000

International Organisation for Standardisation (ISO)

- Publishes internationally recognised standard guidelines that provide a framework for organisations to improve their quality, safety, and efficiency
- These standards are created through a collaborative process involving experts globally and they cover a vast range of industries and topics:
 - ISO 9001:2015 Quality Management Systems
 - ISO 14001:2015 Environmental Management Systems
 - ISO 45001:2018 Occupational Health and Safety
 - ISO/IEC 27001:2022 Information Security, Cybersecurity

ISO/IEC 27000

- Information Security Management System (ISMS):

Document	Function	Topic
ISO/IEC 27000	Standard	Overview
ISO/IEC 27001	Standard	Information Security Management Systems
ISO/IEC 27002	Guideline	Information Security Controls
ISO/IEC 27003	Guideline	ISMS implementation guidance
ISO/IEC 27004	Guideline	Monitoring, measurement, analysis and evaluation
ISO/IEC 27005	Guideline	Guidance on managing information security risks
ISO/IEC 27006	Guideline	Requirements for bodies providing audit and certification of ISMS
ISO/IEC 27007	Guideline	Guidelines for ISMS Auditing
ISO/IEC 270xx	...	...
ISO/IEC 27035	Guideline	Incident Management
ISO/IEC 27701	Standard	Extension for privacy information management

- Evolving list with new 27000 series documents being added to take account of changing needs, for example ISO/IEC 27017 covers Information security management for cloud systems.

Annex SL

- Common framework and High-Level Structure (HLS)
 - Clause 1 Scope
 - Clause 2 Normative References
 - Clause 3 Terms and Definitions
 - Clause 4 Context of the Organisation
 - Clause 5 Leadership
 - Clause 6 Planning
 - Clause 7 Support
 - Clause 8 Operation
 - Clause 9 Performance Evaluation
 - Clause 10 Improvement.

ISO/IEC 27001 Clauses

- ISO/IEC 27001 applies the Annex SL Framework.
 - Clause 1 Scope
 - Clause 2 Normative References
 - Clause 3 Terms and Definitions
 - Clause 4 Context of the Organisation
 - Clause 5 Leadership
 - Clause 6 Planning
 - Clause 7 Support
 - Clause 8 Operation
 - Clause 9 Performance Evaluation
 - Clause 10 Improvement.



Annex A Control Points

Control Points in ISO27001:2022

- A CP, in ISO/IEC 27001, is a specific activity or measure that can be implemented to mitigate a security risk. Control points can be technical, organisational, or procedural. They can be implemented at the individual, departmental, or organisational level.
- CPs are grouped into four themes:
 - Organisational
 - People
 - Physical
 - Technological.

Control Points examples

Organisational Controls	• Governance, Policy and Management Responsibilities • External Collaboration and Threat Management • Information and Asset Management • Incident Management and Business Continuity • Legal, Compliance and Data Protection
People Controls	• Secure Hiring and Onboarding • Awareness, Training and Performance • Remote Work and Off-boarding
Physical Controls	• Physical Access and Perimeters • Threat and Environmental Protection • Asset Management and Use • Equipment Lifecycle and Disposal
Technological Controls	• Access Control and Authentication • Data Protection and Resilience • System and Infrastructure Management • Network Security • Secure Development and Change Management

Key characteristics of a CP

- It should be relevant to the specific risk that it is intended to mitigate.
- It should be measurable, so that the organisation can assess its effectiveness.
- It should be affordable and achievable for the organisation.
- It should be integrated with other controls in the organisation's ISMS.



OT Cyber-Physical Breach Challenge

Scenario: Water Treatment Plant Override

- **Objective:** Analyse an OT security breach, identify security failures, and map them to ISO 27001:2022 Annex A Control Points.
- The 4 Control Themes:
 - **Organisational (Clause 5):** Policies, incident response, governance, continuity.
 - **People (Clause 6):** Training, awareness, reporting, post-employment / contractor rules.
 - **Physical (Clause 7):** Entry security, clear screen/desk, equipment protection.
 - **Technological (Clause 8):** Network segregation, access control, malware protection, logging.
- Your Team's Mission (10 Mins): Read the 3-phase scenario on your handout. Identify every security gap and determine which specific ISO Annex A control point should have prevented it.

Scenario: Water Treatment Plant Override

- Phase 1: Physical & Access
 - Contractor enters server room via a broken, propped-open door.
 - Unattended Engineering Workstation (EWS) left logged in with admin privileges.
- Phase 2: Technical & Malware
 - Unauthorised USB plugged into EWS; malware alters PLC configurations.
 - Flat OT network allows malware to spread; fake operational data sent to monitoring console.
- Phase 3: People & Response
 - Operator sees analogue gauge fluctuations, assumes sensor error, and doesn't report it.
 - No OT incident plan; breach discovered 2 months later during an audit.

Scenario: Water Treatment Plant Override

- Phase 1: Physical & Access

Serial	Vulnerability Identified	ISO Theme	ISO Control Point
1.	Propped/broken door to server/HMI room	Physical	A7.2 (Physical entry controls) A7.3 (Securing offices, rooms, and facilities)
2.	Unattended EWS left logged in with admin privileges	Physical and Technological	A7.7 (Clear desk and clear screen) A8.2 (Privileged access rights)

Scenario: Water Treatment Plant Override

- Phase 2: Technical and Malware

Serial	Vulnerability Identified	ISO Theme	ISO Control Point
1.	Use of unauthorised USB drive	Technological & Physical	A7.10 (Storage media) A8.7 (Protection against malware)
2.	Flat plant network	Technological	A8.22 (Network segregation) A8.20 (Network security)
3.	Spoofed data / No network filtering or log monitoring	Technological	A8.15 (Logging) A8.16 (Monitoring activities)

Scenario: Water Treatment Plant Override

- Phase 3: People and Incident Response

Serial	Vulnerability Identified	ISO Theme	ISO Control Point
1.	Operator ignored anomaly & didn't report it	People	A6.3 (Awareness, education, and training) A6.8 (Information security event reporting)
2.	No OT incident management plan	Organisational	A5.24 (Information security incident management planning) A5.36 (Compliance review)

Question?

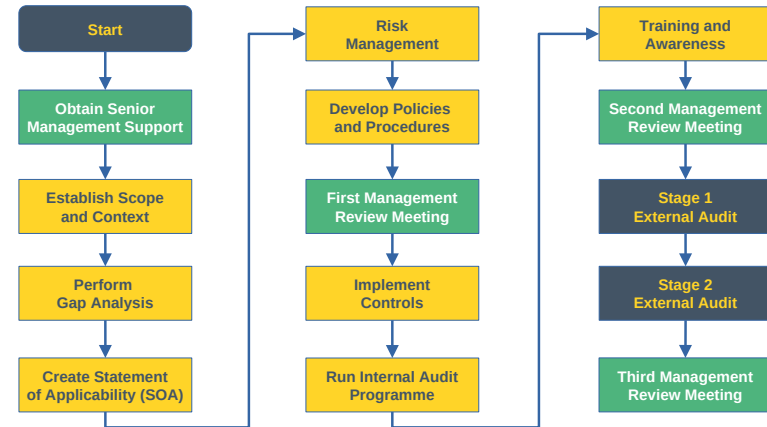
- Why is physical security (Clause A7) just as critical as technological security (Clause A8) in an Operational Technology (OT) environment?

Question?

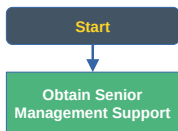
- Why is physical security (Clause A7) just as critical as technological security (Clause A8) in an OT environment?
- In OT, physical access equals logical access. If an attacker or unauthorised individual gets direct physical access to an HMI terminal, EWS, or network switch in a facility, they can bypass perimeter firewalls and technical software controls, allowing them to directly alter physical processes (e.g., valves, chemical levels, power grids) with catastrophic real-world safety impacts.

ISMS Lifecycle & Implementation Strategy

ISO/IEC 27001 - Project

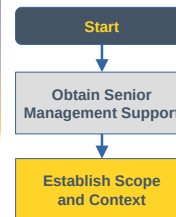


Obtain Senior Management Support



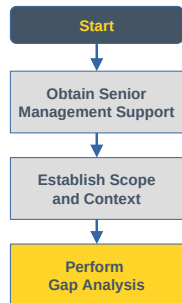
- Identify and Quantify Business Risks.
- Link ISO 27001 to Key Business Drivers.
- Develop a Clear Business Case and Roadmap.
- Engage and Educate Key Stakeholders.
- Present a Clear Call to Action.

Understand the Context of the Organisation



- Understand the Context of the Organisation.
- Hold a kick-off meeting.
- Define the Scope (of the ISMS).
- Identify the, project, Management Review Team (MRT).
- Define the ISMS Objectives.
- Create Internal and external issues register.
- Create Special interest groups register.

Perform Gap Analysis



- Pinpoint the differences between an organisation's existing security practices and the requirements of the ISO/IEC 27001 standard.
 - Audit existing documentation:** to see what's already in place and what needs to be created or updated.
 - A readiness checklist:** is a valuable tool for this audit, helping to systematically identify missing or incomplete policies, registers, and procedures.

Document Type	Document Name	Exists (Y/N)	Notes
Policies and Standards	Information Security Policy		
	Acceptable Use Policy		
	Access Control Policy		

INSPIRING FUTURES

setu.ie | 25

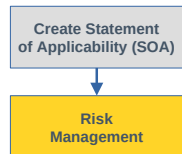
Statement of Applicability



- The SoA is a mandatory document that directly results from the gap analysis.
- It lists all the Security Controls from Annex A.
- For each control, the SoA indicates if it has been implemented, provides a justification for its inclusion, or explains the rationale for its exclusion.
- Formal record of the organisation's risk treatment plan.

No.	Chapter	Topic	Control	Applicable to our organisation (yes/no)	Justification for inclusion	Motivation for non-applicability	Implemented in our organisation (yes/no)
5.1	Organisational controls	Policies for information security	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.				
5.2	Organisational controls	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organisation needs.				

Develop a Risk Management Process



- ISO/IEC 27001 does not mandate a specific methodology (ISO/IEC 27005, ISO 31000 mentioned).
- Focus on identifying, analysing, and treating risks by considering the potential for threats to exploit vulnerabilities.
- The Asset and Risk Register is a central record to track assets, assess risks, and link them to the SoA.
- The register has four key parts:
 - Asset Management
 - Risk Assessment
 - Mapping Risk to SoA
 - Organisation.

INSPIRING FUTURES

setu.ie | 27

Draft or Update Information Security Policy (ISP)

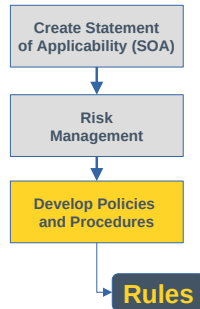


- Context, Objectives and Scope.
- Stakeholder analysis.
- Leadership, Resources, Awareness and Training.
- Operations.
- Performance Evaluation and Continuous Improvement.

INSPIRING FUTURES

setu.ie | 28

Draft or Update Information Security Rules (ISR)



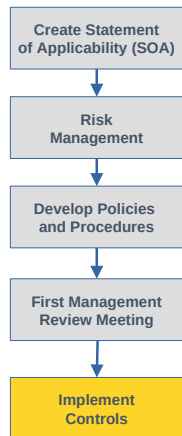
- Translates the ISP into practical Rules.
 - **Organisational**
 - Information classification (A5.9)
 - Bring your own device rules and use of private email accounts (A5.10)
 - Using and storing passwords (A5.17)
 - Using Personally Identifiable Information (A5.34)
 - **People**
 - Security awareness training (A6.3)
 - End of contract/employment (A6.5)
 - Working from home (A6.7)
 - Reporting incidents and vulnerabilities (A6.8)
 - **Physical**
 - Clean desk and clear screen policy (A7.7)
 - **Technological**
 - Phones, tablets and other mobile devices (A8.1)
 - Use of safe networks (A8.21)
 - Use of Cryptography (A8.24)

Hold First Management Review Team Meeting



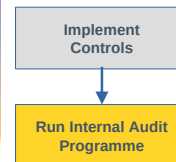
- Formal meeting with Senior Management to launch ISMS implementation project.
 - Re-confirm the scope and Approve it.
 - Define/Agree SMARTER Objectives / objectives and measures and approve them.
 - Review and approve the initial Risk Assessment and the Risk Treatment Plan.
 - Endorse the ICP and other key documents.
 - Commit the necessary resources (personnel, budget) to the project.

Implement Controls



- Put the security plans into action by implementing the specific security controls listed in the SoA and the risk treatment plan.
- The work includes deploying new technical security solutions.
- The ultimate goal is to build a robust security posture, mitigate the identified risks, and close the gaps discovered during the initial analysis.

Run an Internal Audit Programme

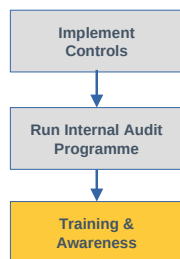


- Create a plan on how to Audit the ISMS.
 - Audit Scope.
 - Audit Criteria.
 - Methodology.
 - Schedule and Resources.
 - Deliverables.

How?

- 1) Define the Scope and Objectives.
- 2) Determine the Audit Team.
- 3) Schedule Activities.
- 4) Develop a Checklist.
- 5) Allocate Resources.
- 6) Establish Reporting.

Training and Awareness



- **Create a plan:** to educate employees on the ISMS, including their specific roles and responsibilities.
- **Detail how information security will be communicated:** throughout the organisation on an ongoing basis.
- **Communicate approved policies:** clearly to all relevant employees.
- **Establish an information dissemination process:** to ensure information is received and acknowledged by everyone.

Second Management Review Meeting



- Start of ongoing, periodic meetings that happen after the ISMS has been established and is operational.
- Agenda focuses on reviewing the effectiveness of the ISMS:
 - Results of internal and external audits.
 - The status of corrective actions from previous reviews.
 - Security incidents and non-conformities.
 - Changes in external and internal issues that affect the ISMS.
 - The performance of security controls and metrics.

Internal Audit



- Annex A controls initially had a high-level audit as part of the process to develop the SoA.
- Conduct a detailed audit which should include:
 - Interviews with Key personnel.
 - Collect evidence and samples from the control area.
 - Collect non-conformities in a Corrective Action Plan (CAP).
- The CAP provides a clear, structured way to address any issues found during an internal audit.
- Fix problems and document the process so it can be proven that it has been handled correctly.

Business Continuity and Disaster Recovery Exercise



- **Plan the Exercise**
 - Define Objectives.
 - Select the Scenario: Common scenarios include:
 - A technology failure, ◦ A physical event, ◦ A cyberattack.
 - Identify Participants.
 - Schedule and Announce.
- **Execute the Exercise**
 - The Kick-Off.
 - The Simulation.
 - Observation.
 - End Ex.
- **Exercise Postmortem**
 - Debriefing.
 - Analyse the Results.
 - Corrective Actions.
 - Update the Plan.



ISO 19011: 7 Principles of Auditing

- ISO 19011 - Guidelines for Auditing Management Systems
- Principles of Auditing
 - Integrity
 - Fair Presentation
 - Due Professional Care
 - Confidentiality
 - Independence
 - Evidence-based Approach
 - Risk-based Approach

INSPIRING FUTURES

setu.ie | 38

Managing the Audit Programme Lifecycle

- **Plan:** Establish the audit programme objectives, scope, and schedule. Identify any risks to the audit itself.
- **Do:** Implement the programme, selecting the audit teams, defining objectives for specific audits, and coordinating the logistics.
- **Check:** Monitor and review the audit programme to see if schedules are being met and if the auditors are actually catching systemic issues.
- **Act:** Improve the programme. Tweak the process, update auditor training, and adjust the schedule based on what was learned.

INSPIRING FUTURES

setu.ie | 39

Information Security Audits

- **ISO 19011 is the Framework**
 - Provides the universal guidelines, core ethics, and the PDCA method for running an audit programme.
- **ISO/IEC 27007 is the Specialisation**
 - Takes generic instruction from ISO 19011 and attaches specific information security context to them.

INSPIRING FUTURES

setu.ie | 40

Stage 1 External Audit – Documentation and Readiness

Stage 1 External Audit

- **High-level review:** of the ISMS documentation is performed to ensure all requirements of the ISO/IEC 27001 standard are met.
- **Auditor examines key documents:** including the SoA, Risk Assessment, and ISP, ISR, etc..
- **Verify the scope of the ISMS:** and confirm the organisation has properly planned its ISMS.
- The audit concludes with a report highlighting any non-conformities; significant issues may cause a delay to the second stage of the audit.

Stage 2 External Audit – Implementation & Effectiveness

Stage 1 External Audit

Stage 2 External Audit

- Comprehensive, on-site review to verify that the ISMS is effectively implemented and operating.
- The auditor will interview staff, review records and logs, and observe daily operations to gather evidence of compliance.
- The audit's outcome determines eligibility for certification, with findings categorised as OFI, Mi-NC, or Ma-NC.
- The organisation must respond to the audit report, addressing each finding, especially major non-conformities, which can prevent certification until resolved.

Third Management Review Meeting

Stage 1 External Audit

Stage 2 External Audit

Third Management Review Meeting

- Review of the Stage 2 Audit Results.
- Status of Certification and Next Steps.
- Planning for Ongoing ISMS Maintenance and Improvement:
 - Assigning resources.
 - Scheduling the next internal audit.
 - Reviewing the risk assessment.
 - Setting new security goals.

Liability and Negligence

• Legal liability

- Legal bound obligation to pay debts.
- A person is said to be legally liable when they are financially and legally responsible for something.
- Bankruptcy.

• Negligence

- A type of delectation or civil wrong.
- The difference between Actions where due diligence is expected and due care as defined in a policy.
- The gap between the policy and best practice or regulation.
- Civil litigation.



General

Document	Year	Body	Specific Purpose
Convention on Cybercrime	2001	CoE	Guideline for any country developing comprehensive national legislation against Cybercrime.
Directive (EU) 2002/58/EC e Privacy Directive	2002	EU	Regulates the processing of personal data and electronic communications.
Regulation (EU) 2019/881 Cybersecurity Act	2019	EU	Formation and powers for ENISA. Framework for Cybersecurity certification of products, services and processes.
Regulation (EU) 2022/9272 Cyber Resilience Act (CRA)	2022	EU	Imposes requirements on manufacturers, importers and distributors to implement appropriate cybersecurity measures on products. Certification scheme.

General

Document	Year	Body	Specific Purpose
Privacy and Electronic Communications (PECR) Regulations	2003	UK	To protect the privacy of individuals and the confidentiality of their electronic communications.
Computer Fraud and Abuse Act (CFAA)	1986	US	To criminalise unauthorised access to computer systems and data, unauthorised modification of data, and DoD attacks.
Bharatiya Nyaya Sanhita [Criminal Code]	2023	India	To criminalise a wide range of offenses, including many that are relevant to cybersecurity, such as cheating, forgery, and defamation.

Data Protection

Document	Year	Body	Specific Purpose
General Data Protection Regulation (GDPR)	2016	EU	To strengthen the protection of personal data in the EU and to give individuals more control over their personal data.
Data Protection Act (DPA) 2018	2018	UK	To protect the privacy of individuals and the confidentiality of their personal data.
Identity Theft and Assumption Deterrence Act (ITADA), 1998	1998	US	To criminalise the unauthorised use of personal information, such as Social Security numbers and credit card numbers.
Information Technology (Amendment) Act, 2008	2008	India	Amended the IT Act, 2000, to add new provisions related to cybersecurity, such as the requirement for certain businesses to appoint a CISO.

Espionage

Document	Year	Body	Specific Purpose
Economic Espionage Act (EEA), 1996	1996	US	To criminalise the theft of trade secrets with the intent to benefit a foreign power.

Financial

Document	Year	Body	Specific Purpose
EU Digital Operational Resilience Act (DORA)	2022	EU	To establish a harmonised framework for digital operational resilience across the financial sector of the EU.
Gramm-Leach-Bliley Act (GLBA), 1999	1999	US	To require financial institutions to implement cybersecurity measures to protect customer data.

Incident Response

SANS

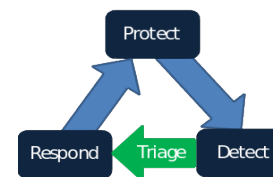
SANS Incident Response Framework



- **Prepare** for an incident before it happens by creating a plan, defining roles and responsibilities, and establishing a CSIRT.
- **Identify** a security incident and determine its nature, scope, and severity by monitoring systems, analysing logs, and collecting evidence.
- **Contain** the incident from spreading and causing further damage by isolating affected systems or taking immediate actions to limit the impact.
- **Eradicate** all traces of it from the environment, including removing malware, patching vulnerabilities, and addressing the root cause.
- **Recover** affected systems to their normal, secure state, which may involve using backups, rebuilding systems, and monitoring.
- **Lessons-Learned** through a post-incident review to understand what happened, what went well, and what could be improved for future incidents.

Forensic Evidence & Incident Investigations

Incident Management



- **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.

Incident Management

- Good source of information are the:
 - **NIST SP 800-61r3** Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile
- Software Engineering Institute (SEI)
 - Handbook for Computer Security Incident Response Teams (CSIRT)

Collection of Digital Evidence

- Evidence is subject to strict rules regarding its admissibility in courts. To be presented, recorded in the court record and considered in the verdict, evidence must be:
- **Relevant**
 - It must pertain to the actual case.
- **Material**
 - It must prove or disprove facts that impact the question before the court.
- **Competent**
 - It must be proven to actually be what it purports to be.

Collection of Digital Evidence

- **Do Not Harm** Do as little as possible beyond disconnecting the system from the network and protecting it until it can be handed over to an Garda Síochána or other law enforcement.
- **Don't turn off** the system as data in volatile memory (RAM) will be lost.
- **Disconnect from the network** as this prevents a hacker from covering their tracks by deleting evidence like log files.
- **Don't use the system** for any reason, like running programs as you may unwittingly overwrite data in memory
- **Don't open files** to examine them as you will modify the access and modify time record on the file.
- **Document everything** you do.

Preservation of Digital Evidence

- **Preserve digital evidence in its original state**
 - Copy it from one machine to another via a private network connection.
 - The source computers memory should be transferred to the target computer first.
 - Source computer hard disk contents should be copied to the target computer as a bit level image not file by file to create an exact copy of the source disk data including empty space.
 - A number of specialist software programs exist for this purpose.



Preservation of Digital Evidence

- A **forensic duplicate** consists of every bit of the raw bitstream stored in an identical format (e.g. using an identical disk).
- On the other hand, a **qualified forensic duplicate** is a copy where every bit of information is still stored, but perhaps in a different form, such as an ISO image.
- Both are permissible as evidence, but the "best evidence" should be used, e.g. the original disk.



Evidence Chain of Custody

- Chain of Custody is the chronological documentation, showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic.
 - Who
 - What
 - When
 - Where
 - How.

Process of Investigation

- Identify:
 - Suspects
 - Systems
 - Witnesses
 - Investigative team
 - Search warrants.
- For filesystems, analyse the ownership and the modification records.
- Means, Opportunity and Motives (MOM). Why?
- Modus Operandi (MO). How?

Interviewing Suspects

- **Plan** the interview.
- Interview or interrogation techniques.
- **Interview**
 - Conducted in a cordial atmosphere where a suspect or witness is more comfortable physically and psychologically.
- **Interrogation**
 - Questioning in an uncomfortable atmosphere under psychological pressure.

Hearsay

- Information gathered by one person from another concerning some event, condition, or thing of which the first person had no direct experience.
- “**hearsay evidence**” in court is generally not allowed.
- **Business entry rule** (US) which is an exception to the hearsay rule.
 - Writings or records of acts, events, conditions, opinions, or diagnosis, made at or near the time by, or from information transmitted by, a person with knowledge are admissible if kept in the regular course of business.
 - The exception allows the record to substitute for the in-court testimony of the employees, but it can only substitute for what the employee could testify about.

Exercise

Quiz

SE TU
Ollscoil
Teicneolaíochta
an Oirdeheiscirt
South East
Technological
University

Icons: A green circle with a white checkmark, an orange circle with a white exclamation mark, and a pink circle with a white question mark.

Convention on Cybercrime

The Additional Protocol to the Council of Europe's Convention on Cybercrime requires State Parties to criminalise which of the following actions?

- A) Requiring manufacturers to provide users with information about product cybersecurity risks.
- B) The mandatory reporting of all data breaches to a supervisory authority within 72 hours.
- C) Establishing a certification framework for Information and Communications Technology (ICT) products and services.
- D) Criminalising the dissemination of racist and xenophobic material through computer systems.

Convention on Cybercrime

The Additional Protocol to the Council of Europe's Convention on Cybercrime requires State Parties to criminalise which of the following actions?

- A) Requiring manufacturers to provide users with information about product cybersecurity risks.
- B) The mandatory reporting of all data breaches to a supervisory authority within 72 hours.
- C) Establishing a certification framework for Information and Communications Technology (ICT) products and services.
- D) **Criminalising the dissemination of racist and xenophobic material through computer systems. ✓**

EU Cyber Legislation

Which EU regulation primarily aims to strengthen the operational resilience of the EU financial sector to digital operational disruptions and threats, applying from January 17, 2025?

- A) DORA
- B) GDPR
- C) CRA
- D) ePrivacy Directive

EU Cyber Legislation

Which EU regulation primarily aims to strengthen the operational resilience of the EU financial sector to digital operational disruptions and threats, applying from January 17, 2025?

- A) **DORA ✓**
- B) GDPR
- C) CRA
- D) ePrivacy Directive

ISO/IEC 27001 Internal Review Scope

An organisation is preparing for its initial internal assessment cycle before external verification. According to Clause 9.2 of the ISO/IEC 27001 standard framework, what specific criteria must be verified during these scheduled internal management audits?

- A) That the system completely matches external data privacy obligations and minimises operational budget requirements.
- B) That the system conforms to organisational requirements and standard criteria while being effectively deployed.
- C) That the system satisfies international trade policies and remains fully compatible with third-party software tools.
- D) That the system focuses exclusively on technical perimeter security and completely automates incident logs.

ISO/IEC 27001 Internal Review Scope

An organisation is preparing for its initial internal assessment cycle before external verification. According to Clause 9.2 of the ISO/IEC 27001 standard framework, what specific criteria must be verified during these scheduled internal management audits?

- A) That the system completely matches external data privacy obligations and minimises operational budget requirements.
- B) **That the system conforms to organisational requirements and standard criteria while being effectively deployed.** ✓
- C) That the system satisfies international trade policies and remains fully compatible with third-party software tools.
- D) That the system focuses exclusively on technical perimeter security and completely automates incident logs.

SANS IRF

According to the SANS IRF, which phase is directly followed by the Eradication phase?

- A) Preparation
- B) Identification
- C) Containment
- D) Recovery
- E) None of the above

SANS IRF

According to the SANS IRF, which phase is directly followed by the Eradication phase?

- A) Preparation
- B) Identification
- C) Containment
- D) **Recovery** ✓
- E) None of the above

Preserving Volatile Digital Evidence During Incidents

An analyst detects an active network intrusion on a corporate system containing sensitive transactional registries. To preserve digital evidence competently for potential future court proceedings, what protocol should be prioritised immediately?

- A) Power down the platform immediately to prevent any further administrative log changes by the remote adversary.
- B) Disconnect the asset from the network while keeping it powered on to protect volatile memory configurations.
- C) Launch internal scanning scripts on the affected host to identify deleted elements and modify storage states.
- D) Open individual application files sequentially to evaluate specific chronological timestamps and verify content data.

Preserving Volatile Digital Evidence During Incidents

An analyst detects an active network intrusion on a corporate system containing sensitive transactional registries. To preserve digital evidence competently for potential future court proceedings, what protocol should be prioritised immediately?

- A) Power down the platform immediately to prevent any further administrative log changes by the remote adversary.
- B) **Disconnect the asset from the network while keeping it powered on to protect volatile memory configurations.** ✓
- C) Launch internal scanning scripts on the affected host to identify deleted elements and modify storage states.
- D) Open individual application files sequentially to evaluate specific chronological timestamps and verify content data.

Learning Outcomes



Learning outcomes

You should now be able to:

- Analyse the Core Architecture of ISO/IEC 27001 and the structural relationship between the Annex SL and the operational security controls of Annex A. ✓
- Describe the end-to-end strategy for transitioning an ISMS from initial project planning to operational readiness, culminating in internal reviews and formal Stage 1 and Stage 2 external certification audits. ✓
- Differentiate between the foundational management auditing principles of ISO 19011 and the specialised cybersecurity requirements of ISO/IEC 27007 to evaluate how compliance evidence is gathered and verified. ✓
- Explain the intersection of cybersecurity with liability law, CNI regulations, and the foundational requirements for preserving a strict chain of custody during digital forensic evidence collection. ✓



Ollscoil
Teicneolaíochta
an Oirdheiscirt
South East
Technological
University



EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach

☎ +353 59 917 5000 | ✉ diarmuid.obriain@setu.ie | setu.ie
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire



Ollscoil
Teicneolaíochta
an Oirdheiscirt
South East
Technological
University

Thank you

engcore
advancing technology

INSPIRING FUTURES