Session 2

📄 From Incident Response to Resilience

“What happens after a company adopts a security policy? How do we ensure it works when a major incident or disruption occurs?”

Part 5 – Incident Response & Supply Chain Security

Why Incidents Matter

- Cost of incidents in EU: €180 billion/year (ENISA estimate).
- Common vectors: phishing, ransomware, DDoS, supply chain compromise.
- EU laws:
  - NIS2 → 24h initial notification, 72h report.
  - DORA → financial firms must classify & report ICT incidents.
  - CRA → connected devices securty-by-design and by-default

ISO/IEC 27002:2022

Incident Management: 4 themes 17 controls

- **Org**: 11 controls
- **Ppl**: 2 controls
- **Phys**: 1 control
- **Tech**: 4 controls
-

ISO/IEC 27002:2022 (Incident Management)

Organisational:

- 5.24 Information security incident management planning and preparation
  - Responsibilities and procedures
  - Reporting information security events
  - Reporting security weaknesses
- 5.25 Assessment of information security incidents and decision taking
- 5.5 Contact with authorities
- 5.29 Information security during disruption

ISO/IEC 27002:2022 (Incident Management)

- 5.6 Contact with special interest groups
- 5.7 Threat intelligence
- 5.26 Information security incident response
- 5.27 Learning from information security incidents
- 5.28 Collection of evidence
- 5.30 ICT readiness for business continuity
- 5.37 Documented operations procedures

ISO/IEC 27002:2022 (Incident Management)

People:

- 6.4 Disciplinary process
- 6.8 Information security event reporting **Physical**:
- 7.4 Physical security monitoring

ISO/IEC 27002:2022 (Incident Management)

Technical:

- 8.8 Management of technical vulnerabilities
- 8.13 Information backup
- 8.15 Logging
- 8.16 Monitoring activities

ISO/IEC 27035:2023 – Information Security Incident Management

Purpose & Context

- It defines principles, processes, and guidance for managing information security incidents.
- It augments the incident management controls in **ISO/IEC 27002**.
- Applicable to all organizations (any size, sector) and external incident management providers.

ISO/IEC 27035:2023 (2)

Structure

- Part 1: Principles & Process
- Part 2: Guidelines to Plan & Prepare
- Part 3: ICT Incident Response Operations
- Part 4: Coordination across organizations

ISO/IEC 27035:2023 (3)

Core concepts

- **Incident Management Team (IMT)**: trusted, skilled group leading the incident lifecycle.
- **Incident Response Team (IRT)**: operational team(s) executing response activities.
- **Incident Handling**: lifecycle covering detection → reporting → assessment → response → learning.

ISO/IEC 27035:2023 (4)

Incident Lifecycle (5 Phases)

Phase	Purpose / Key Activities
Plan & Prepare	Define policy & governance, establish IMT/IRT, ensure tools & training are in place, perform exercises.
Detect & Report	Monitor, detect anomalies/events, report potential incidents from internal/external sources.

Assess & Decide	**Triage events to confirm incident status, understand scope, determine severity, assign response paths.**
Respond	Contain, investigate, eradicate the root cause, recover impacted systems, preserve evidence as needed.
Learn Lessons	Review what went well/poorly, implement improvements, update policies, train, report to stakeholders.

Roles & Responsibilities in IR

- IR Team: SOC analysts, CISO, Legal, Communications, IT Ops.
- Management board → accountable under NIS2.
- External: CSIRTs, regulators, suppliers.

Supply Chain Risks in Incidents

- 60–70% of major incidents stem from suppliers (SolarWinds, MOVEit).
- CRA requires vulnerability handling and secure-by-design.
- ISO/IEC 27002:2022 controls: supplier agreements, outsourced ICT services.
- ISO/IEC 27036 (supplier relationships).

Case Study – Automotive Supplier Breach

- Attack: malware in embedded automotive software → vehicle recalls.
- Regulatory obligations: CRA (product security), NIS2 (critical supplier reporting).
- Standards: ISO 27036 (supplier risk), ISO 27035 (incident response).

Applied Discussion

- Question: “As the CISO of a European car manufacturer, what 3 measures would you add to your supplier policy to reduce risks?”

- Possible answers:
  - Mandatory SBOM delivery.
  - Incident notification clauses.
  - Annual supplier audits.

What is an SBOM?

SBOM - Definition & Purpose

- **SBOM = Software Bill of Materials**
  - A *structured inventory* of all components (libraries, dependencies, modules)
- Inspired by **supply chain management**
- Shall provides **visibility** into:
  - Open-source and third-party dependencies.
  - Versions and licensing information.
  - Known vulnerabilities.

SBOM - Why It Matters

- **Transparency**: Understand what's inside critical software.
- **Vulnerability management**: Faster detection & response to newly disclosed CVEs.
- **Compliance**: Supports license management and regulatory reporting.
- **Supply chain trust**: Essential for secure procurement and vendor risk management.

SBOM Standards & Practices

- **SPDX (Software Package Data Exchange) –** ISO/IEC 5962:2021, machine-readable format.
- **CycloneDX –** Lightweight BOM format from OWASP, widely adopted in DevSecOps.
- **SWID Tags –** Software Identification Tags (ISO/IEC 19770-2).

SBOM - Integration into Security

- **Development pipeline**: SBOMs generated during CI/CD (DevSecOps).
- **Runtime monitoring**: SBOMs can feed into vulnerability scanners & asset management.
- **Incident response**: Enables rapid assessment of exposure to vulnerabilities (e.g., Log4Shell).
- **Compliance**: Helps meet ISO/IEC 27036 (supplier security) and NIST guidelines.

Part 6 – Privacy & AI

ISO/IEC 27002:2022 (Privacy)

Only 3 (org) controls:

- **5.34 – Protection of PII within information security management**
- **5.32 – Data leakage prevention**
- **5.35 – PII and privacy obligations in supplier relationships**

ISO/IEC 27002:2022 (AI)

No AI-specific controls, some *general-purpose controls apply to AI contexts*

- **5.23 – Information security for use of cloud services** → many AI services are cloud-based.
- **8.10 – Secure development lifecycle** → applies to AI/ML model development, training data, and deployment.
- **8.11 – Secure coding** → can be extended to ML pipelines.
- **5.36 – Compliance with security requirements** → could cover AI regulations indirectly.

ISO/IEC 27701 – Privacy & GDPR

- Extends ISMS into PIMS (Privacy ISMS).
- GDPR obligations: data minimization, lawful processing, breach notification.
- Example: healthcare provider facing a patient data breach.

ISO/IEC 42001 & EU AI Act

(under development)

- AI Act: high-risk AI must be robust, transparent, and secure.
- ISO 42001: first management standard for AI systems.
- Example: medical AI misclassification → liability & regulatory action.

- **ISO/IEC 23894:2023** → *AI risk management* (complements 27005's risk approach, but specialized for AI).
- **ISO/IEC 38507** → Governance implications of AI for organizations.

Exercise

- Case: AI recruitment startup flagged by regulator.
- Task: Groups identify:
  - EU obligations (GDPR, AI Act…).
  - ISO standards (27701, 42001…).
  - 3 compliance priorities for the company's policy.

Part 7 – Business Continuity & Resilience

ISO/IEC 27002:2022 (continuity)

- **5.29 – ICT readiness for business continuity**
- **5.30 – ICT continuity (BCP)**
- **5.31 – Lessons learned from information security incidents**

ISO/IEC 22301:2019 – Business Continuity

- Defines **requirements** to plan, establish, implement, operate, monitor, review, maintain, and continually improve a BCMS.
- Certifiable standard (like 27001)

ISO/IEC 22301:2019 (2)

Core Elements

1. **Context of the organization –** Identify critical activities and stakeholders.
2. **Leadership & governance –** Assign roles, responsibilities, top management commitment.
3. **Business Impact Analysis (BIA) –** Identify dependencies, recovery priorities, and impacts of disruption.
4. **Risk assessment & treatment –** Evaluate threats and vulnerabilities (aligns with ISO/IEC 27005).

ISO/IEC 22301:2019 (3)

Core Elements (2) 5. **Continuity strategies & solutions –** Define RTOs (Recovery Time Objectives), RPOs (Recovery Point Objectives), redundancy, alternate sites, cloud failover, etc. 6. **Incident response structure –** Crisis communication, escalation, emergency response. 7. **Testing & exercises –** Regular validation of BCP and DRP plans. 8. **Performance evaluation –** KPIs, audits, and management reviews. 9. **Continuous improvement –** Lessons learned, corrective actions, resilience culture.

Continuity vs. Recovery

- Business Continuity: **maintaining** essential services.
- Disaster Recovery: **restoring** IT infrastructure.

Domain	Main Standard	Focus
ICT Disaster Recovery	**ISO/IEC 27031**	Ensures readiness and recovery of information and communication systems.
Overall Business Continuity	**ISO 22301**	Framework for continuity management (organization-wide).
Incident & Crisis Response	**ISO 22320**	Managing emergency response and crisis coordination.
Technical Guidance (BIA, Supply Chain, etc.)	**ISO/TS 22317**, **22318**	Supporting processes for continuity and recovery.

Group Exercise – Cloud Continuity Plan

- Task: Define 3 continuity measures for a cloud provider
    - Map measures to standards + regulatory duties.

Example

1. Geo-redundancy backup.
2. Crisis comms plan.
3. Service level objectives (RTO, RPO).

Case Study – Cloud Service Provider

- Data center outage → customers offline.
- Obligations: NIS2 (essential service), DORA (critical ICT provider).
- Standards: ISO 22301 (BCMS), ISO 27001 (ISMS).

Part 8 – Conclusions & Homework

Integration: Policy Cycle + ISO + EU Law

- EU laws = rules.
- ISO = operational guidelines.
- Companies = organisations implementing.
- Staff/budgets = resources.

Policy Trade-offs in Cybersecurity

- Security vs. Innovation (AI Act).
- Compliance cost vs. resilience (CRA for SMEs).
- Transparency vs. liability (NIS2 reporting).

Evaluation & Maintenance

- Policy cycle & analysis
- ISO 27001 PDCA = continual improvement.
- EU laws evolve (NIS → NIS2).
- Companies should plan policy reviews annually or after incidents.

Group Reflection

- Question: “Which EU regulation will most transform your industry in the next 5 years, and why?”

Homework Briefing

- Deliverable: Policy Brief (3–5 pages or 5–10 slides).
- Audience: Board of directors or regulator.
- Must include:
    1. Problem definition.
    2. Policy cycle stages.
    3. (EU) law → (ISO) mapping.
    4. Policy options & trade-offs.
    5. Stakeholders (internal/external).
    6. Adoption & continuity measures.

=> https://pst.libre.lu <=

=> pst@libre.lu <=