Session 1

📄 Policy Framework, EU regulations & ISO Foundations

Part 0 – Introduction

Policy Framework, EU regulations & ISO Foundations

- *Objectives*:
  - Understand EU cybersecurity regulatory landscape.
  - Learn how international standards (ISO) provide governance structures.
  - Frame cybersecurity as part of a broader policy cycle.

Please introduce yourself

- Who are you?
- What you do, why you take this Masterclass?
- Expectations for career in cybersecurity

Whoami

- Pascal Steichen (physicist with a tech/cyber angle)
- CEO at LHC ; Chair of ECCC
- Member of the CIC-CPCS ; the CRH SC & the OLAS CA
- Lecturer for MISSM and MTECH

Ice-breaker exercise

- **Scenario**: "You are the new CISO of a European bank. The CEO asks: Are we compliant with EU cybersecurity law?"
- **Task**: In small groups (5–7 min), identify 3 laws/regulations that might apply.

Debrief

- is that the work of a policy-maker?
- what is a policy?
- what type of policies exist?
- why do we need policies in cybersecurity?

Part I – EU Cybersecurity & AI - Policy Context

Why Cybersecurity Matters

- Tech dependency of our society
- Cybersecurity == public value (trust, safety, resilience).
- More and more incidents:
  - ransomware in healthcare,
  - logistics disruption,
  - AI misuse.

ENISA Threat Landscape 2025

- Most targeted (38,2%): **Public administration**
- 77% of incidents: **DDoS**
- **Ransomware**: most impactful threat
- **Hacktivism** (ideology-driven) drove most incidents
- Main **entry points**: Phishing (60%) and vulnerability exploitation (21.3%)
- **State-aligned** groups intensified operations

The EU Legal-Policy Ecosystem

- NIS2 (2022/2555) → Essential entities, board accountability, incident reporting.
- DORA (2022/2554) → ICT operational resilience in financial sector.
- CRA (2024 adoption) → Secure-by-design ICT products, vulnerability handling, SBOM.
- EU AI Act (2024) → Risk-based classification, robustness, cybersecurity for high-risk AI.
- ...

Supervisory Bodies & Institutions (e.g. NIS2)

- **EC/ENISA**: strategic guidance, threat landscape reports, EU coordination.
- **CSIRT Network**: operational defense, information sharing.
- **Coordination Group** (regulators): policy execution, incident registration and sanctions
- **CyClone** (crisis organs): emergency coordination, crisis management, temporary measures

---

What is a policy?

A set of decisions authorized by legitimate stakeholders that generate/allocate/shift resources with the intent to create value

---

Policy as Governance System

- From public policy theory: policy requires 4 components:
    1. **Rules** (laws, directives, standards..).
    2. (operational) **Guidelines** (ISO standards, ENISA guidance...).
    3. **Organisations** (CSIRTs, regulators, corporate/group policies..).
    4. **Resources** (budget, expertise, staff...).

Example:

1. CRA (rule)
2. → ISO 27002 5.19-5.23 (guidelines)
3. → ENISA, ICT vendors (orgs)
4. → engineers & budgets (resources).

Exercise – “Match Regulation to Industry”

- Energy provider
- Insurance
- IoT vendor
- Recruitment startup

Exercise – “Match Regulation to Industry”

- Energy provider → *NIS2*.
- Insurance → *DORA*.
- IoT vendor → *CRA*.
- Recruitment startup → *AI Act*.

Key policy concepts

Policy cycle: the process through which policies are developed, implemented, evaluated and maintained by relevant stakeholders

Policy analysis:

- *Ex-ante*: investigating available options for new policies when the organisation is facing a problem/opportunity.
- *Ex-post*: investigation the implementation and/or the effects of existing policy.

Key policy concepts (2)

- **Policy issue**: a problem or challenge that requires a policy response
- **Policy response**: strategy/action that is adopted in reaction to an issue or opportunity
- **Policy options**: the different options available to address a specific issue or opportunity
    - **assessment criteria**: used to assess the quality of a policy option/alternative (cost-efficiency, effectiveness, political support, etc.)

Key policy concepts (3)

- **Policy intentions**: specific objectives that a policy is designed or expected to achieve
- **Policy mix** (package): the combination of different policies that are implemented together to achieve a common goal
- **Policy gap**: discrepancy between the existing policy outcomes and the desired expected results
- **Policy failure**: when a policy does not achieve its intended outcomes

---

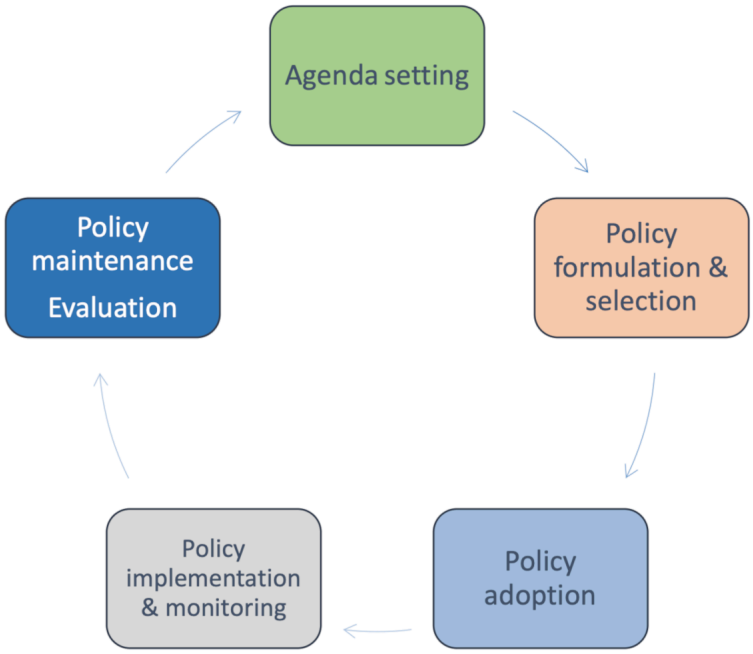
Key policy concepts (4)

- **Policy trajectory**: how policy directions are shaped during implementation. As a result, outcomes might differ from one area to another implementation area
- **Evidence-based policy making**: rigorous evidence to inform and guide policy decisions
- **Policy framing**: the use of specific frameworks, ideologies, beliefs and values to advocate for a particular agenda by shaping the narrative around issues and the policy (*the contrary of evidence-based policy making!*)

Key policy concepts (5)

- **Policy trade-offs**: maximization vs optimization (best option based on the constraints!)
    - **Policy effects** on stakeholders: policy has + and - effects, and it may affect stakeholders in different ways. Policymakers must balance competing interests, priorities, and objectives
    - **Criteria**: efficiency and participation

Policy Cycle (simplified)



Put in the cyber context

1. **Agenda-setting** → attacks & societal pressure.
2. **Formulation** → EC / Ministries / Dept. drafts proposals.
3. **Adoption** → Parliament / Board approve.
4. **Implementation** → eu/national laws / company ISMS.
5. **Evaluation** → regulator reviews, new laws (e.g. NIS → NIS2) / PDCA.

Part 2 – Policy Cycle & ISO PDCA

---

1. Agenda Setting

Refers to the process by which certain issues/opportunities gain attention within the public/internal discourse, influencing the attention or priorities of all types of stakeholders (board, shareholders, clients, partners, internal departments, staff)

Who determines the policy agenda?

- Government and political leaders
- Clients, shareholders
- Internal departments, subsidiaries
- Partners, suppliers
- Interest groups, lobbies and advocacy coalitions
- Media and public opinion

---

2. Policy formulation

- Defining the **objectives** of the policy
- Developing and selecting the policy **option(s):** how to achieve those objectives?

How?

- Assessing policy options against **criteria** (ex: costs-efficiency, etc.)
- Balancing **competing interests** of different stakeholders (trade-offs)

- Minimizing the potential **unintended consequences** of the policy

---

Criteria

- Legality
- Acceptability
- Operational ease
- Effectiveness
- Cost-efficiency
- Sustainability
- Ethical/equity

ISO/IEC Standards as Policy System

- ISO/IEC 27001: ISMS backbone.
- ISO/IEC 27002: 93 security controls.
- ISO/IEC 27005: risk management.
- ISO/IEC 27035: incident management.
- ISO/IEC 27036 (supplier security).
- ISO/IEC 27034 (application security).
- ISO/IEC 27701: privacy extension.
- ISO/IEC 42001: AI governance.

Integration Example: CRA

- **Agenda**: secure-by-design products.
- **Formulation**:
  - ISO/IEC 27036 (supplier security).
  - ISO/IEC 27034 (application security).
- **Policy cycle**: Regulation → Adoption → Implementation → Evaluation

---

3. Policy Adoption

Formal approval by *relevant entities*

1. Rules (terms of references, contracts...)
2. Operational guidelines (standards, reference implementations...)
3. Organisation(s) and processes (procedures, desk instructions...)
4. Resources: expertise, HR, technology, etc. (measures and actions)

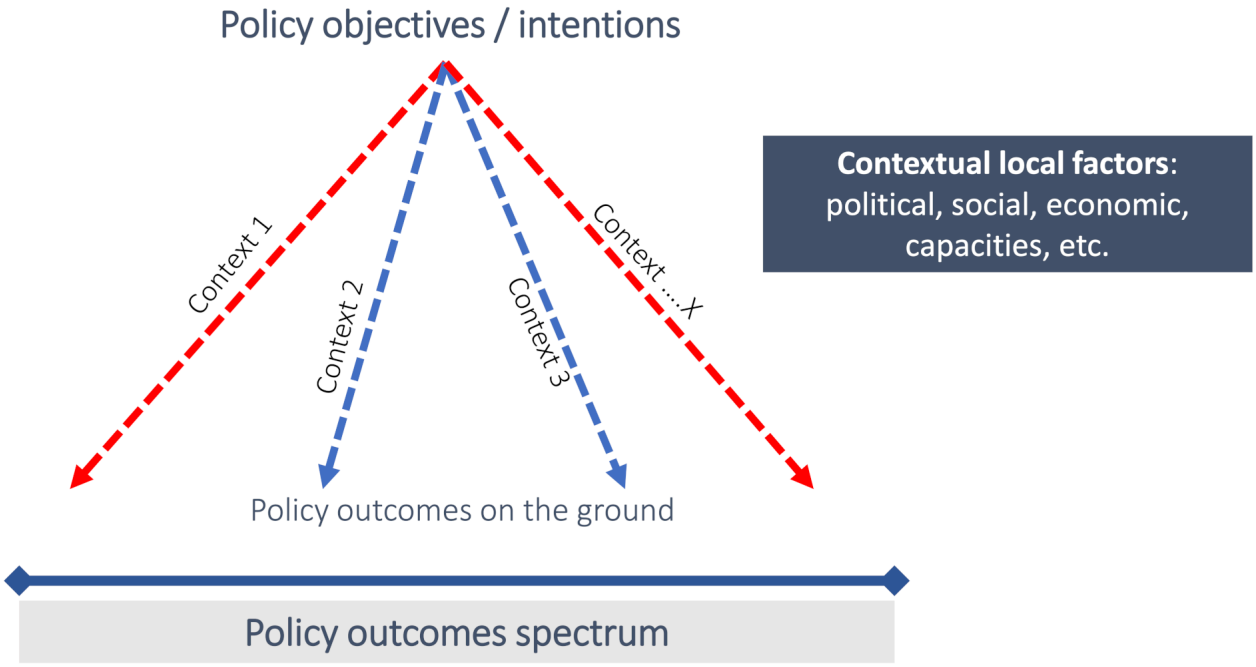
---

4. Implementation

Putting the chosen policy into action:

- Deliver services
- Build new infrastructures
- Create new departments / services / products
- Recrute new expertise
- Etc.

Policy trajectory



---

5. Policy Evaluation & Maintenance

Policy evaluation

- It determines whether the policy has achieved its **desired effects** (outcomes/impacts) and assess **unintended consequences**
- Policy evaluation provides the evidences-based data to take the **corrective measures** to improve policy **efficiency** and **effectiveness**

Policy maintenance

- Ensuring that the policy remains **relevant**, **efficient** and **effective**
  - Addressing potential **weaknesses**, shortcomings, unintended effects
  - **Update** the policy with new legal and regulatory requirements, best practices, etc.
- Keeping stakeholders **informed** progress, challenges, etc

---

Methods for policy evaluation

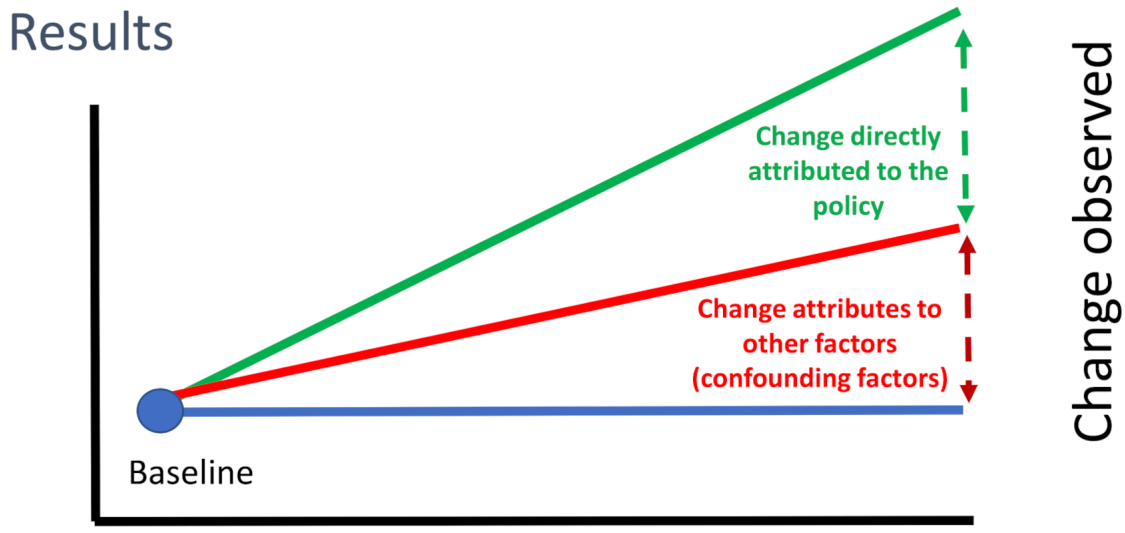
Quantitative evaluation

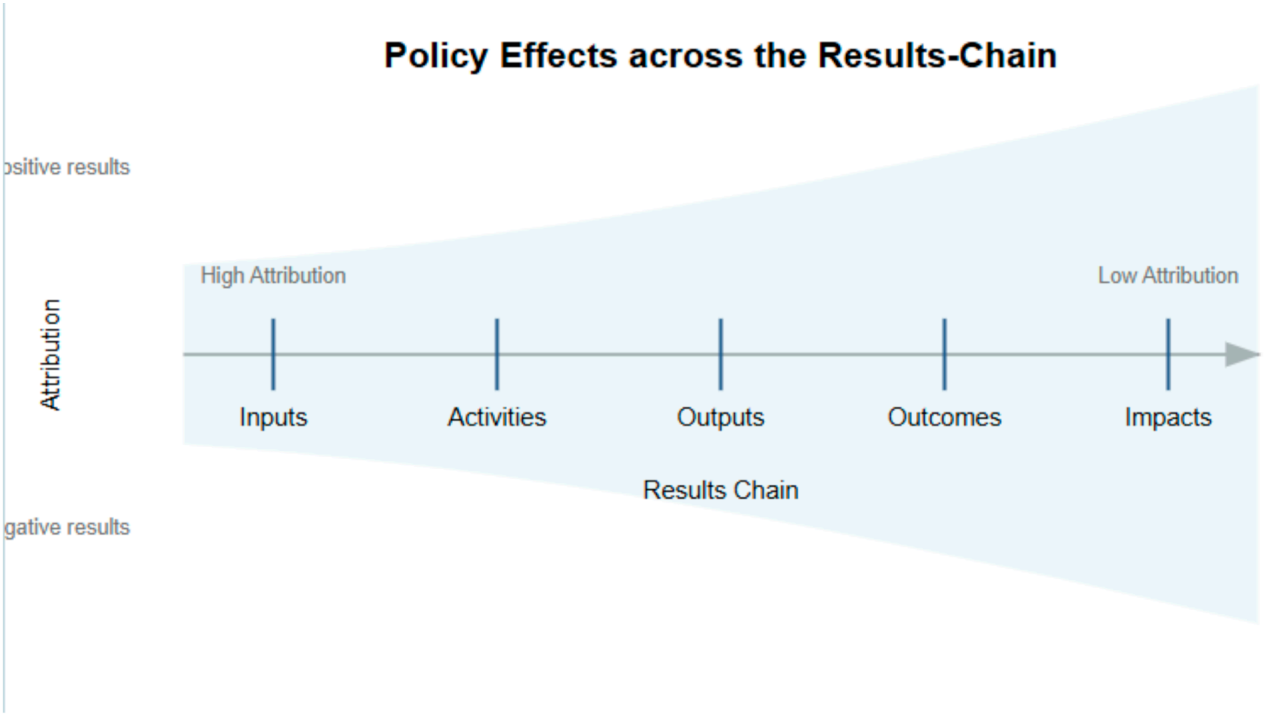
- **Cost-benefit** analysis: assigning monetary values to tangible and intangible factors
- **Impacts** evaluation: to which extent the improvement can be attributed to the policy using a control and a treatment gr
  - treatment group: participants are randomly assigned
  - control group: participants are not randomly assigned

Qualitative evaluation

- In-depth qualitative analysis of the policy: positive, negative, and unintended results
- Critical review of the **change(s) observed**

Policy effects and Result Chain





Part 3 – ISO/IEC toolbox & Focus Areas

ISO/IEC 27000 Family Overview

- **suite of standards** covering information security management in a modular way.
- **27000** is like the "glossary and map" of the family—defining the terms and concepts.
- **27001** is the **only certifiable "requirements" standard** for an ISMS.
- **27002** provides the **detailed catalogue of controls** (== Annex A of 27001). Think of it as the "implementation handbook."

- **27004 –** Monitoring, measurement, analysis & evaluation of the ISMS (metrics & KPIs).

- **27005** dives deeper into **risk management**, essential since 27001 requires a risk-based approach
- **27006 –** Requirements for certification bodies auditing and certifying ISMS.

- **Sector-specific**: (27017, 27018, 27701, etc.) help adapt the ISMS to **privacy, cloud environments, energy, supply chains**. This shows the family's ability to **evolve with new challenges**.

ISO/IEC 27002:2022

Themes (categorisation of controls): a) people, b) physical, c) technological, d) organisational.

ISO/IEC 27002:2022 (2)

Attributes:

1. **Control type -** perspective of when and how the control modifies the risk
2. **Information security property -** characteristic of the information to be preserved
3. **Cybersecurity concept** (ref. ISO/IEC TS 27110)
4. **Operational capability -** practitioner's perspective
5. **Security domain**

ISO/IEC 27002:2022 (3)

1. Control types
    - **Preventive** (the control that is intended to prevent the occurrence of an information security incident),
    - **Detective** (the control acts when an information security incident occurs) and
    - **Corrective** (the control acts after an information security incident occurs).
2. Information security properties
    - **Confidentiality**,
    - **Integrity**, and **Availability**.

ISO/IEC 27002:2022 (4)

3. Cybersecurity concepts
    - **Identify**,
    - **Protect**,
    - **Detect**,
    - **Respond**,
    - **Recover**.

ISO/IEC 27002:2022 (5)

4. Security domains
    - **Governance and Ecosystem**
    - **Protection**
    - **Defence**
    - **Resilience**

ISO/IEC 27002:2022 (6)

5. Operational capabilities
    - **Governance,**

    - **Asset_management,**
    - **Information_protection,**
    - **Human_resource_security,**
    - **Physical_security,**
    - **System_and_network security,**
    - **Application_security,**
    - **Secure_configuration,**
    - **Identity_and_access_management,**

- **Threat_and_vulnerability_management,**
- **Continuity,**
- **Supplier_relationships_security,**
- **Legal_and compliance,**
- **Information_security_event_management, and**
- **Information_security_assurance.**

ISO/IEC 27001 vs. 27002

- “What” vs. “How”.

Part 4 – Group Exercise

Group Work

- Groups of 3 people
- Case study: Hospital, Automotive supplier, AI-powered Fintech, Energy powerplant, Meat supplier
- Tasks:
    - Map applicable EU law.
    - Identify ISO standards.
    - Detail out the agenda-setting
- Prepare 2–3 slides.

---

1. **Rules** (laws, directives, standards..).
2. (operational) **Guidelines** (ISO standards, ENISA guidance...).
3. **Organisations** (CSIRTs, regulators, corporate/group policies..).
4. **Resources** (budget, expertise, staff...).

- **Policy cycle**: Agenda-setting → Formulation → Adoption → Implementation → Evaluation

---

Agenda-setting

Refers to the process by which certain issues/opportunities gain attention within the public/internal discourse, influencing the attention or priorities of all types of stakeholders (board, shareholders, clients, partners, internal departments, staff)

Presentations

- 10 min per group.
- Discussion
