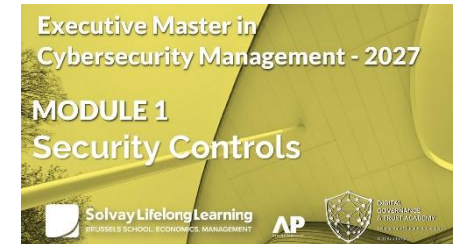


Module M1 Alignment Dashboard Across All 12 ECSF Roles

Below is the graphical representation of how Solvay Business School's **Module EMCM M1** aligns with the **12 European Cybersecurity Skills Framework (ECSF)** role profiles, categorized by primary Key Knowledge (KK) coverage and cognitive depth [15, 16, 45–48].



Tier 1: Core Governance, Legal & Strategy Roles (Highest Alignment)

- **Cyber Legal, Policy & Compliance Officer** [100% Primary Alignment] [██████████] 5/5 Primary KK Items
 - **Primary Cognitive Levels: Evaluate / Create / Apply**
 - **M1 Core Topics:** NIS2 Directive, DORA, Cyber Resilience Act, GDPR Article 35 DPIA, and legal control mapping.
- **Cyber Incident Responder** [85% Primary Alignment] [██████████ 1/2] 11/13 Primary KK Items
 - **Primary Cognitive Levels: Apply / Analyze / Evaluate**
 - **M1 Core Topics:** Incident handling standards, 24h/72h breach notification, SIEM/EDR, and CSIRT/SOC operations.
- **Chief Information Security Officer (CISO)** [82% Primary Alignment] [██████████] 9/11 Primary KK Items
 - **Primary Cognitive Levels: Evaluate / Analyze / Create**
 - **M1 Core Topics:** ISO 27001 policies, CyFun maturity levels (1–5), 33 Control Domains, and executive board governance.
- **Cybersecurity Risk Manager** [80% Primary Alignment] [██████████] 8/10 Primary KK Items
 - **Primary Cognitive Levels: Analyze / Evaluate / Apply**

- **M1 Core Topics:** ISO 31000/27005, Bow-Tie threat modeling, FAIR risk scoring, and Risk Registers.
-

● Tier 2: Technical, Operational & Analytical Roles (Strong Alignment)

- **Penetration Tester** [83% Primary Alignment] [██████████ 1/2] 10/12 Primary KK Items
 - **Primary Cognitive Levels:** Apply / Analyze / Create
 - **M1 Core Topics:** Multi-stage attack chains, PTES/OWASP testing, exploit scripting, and 'Assume Compromise' red teaming.
- **Cybersecurity Auditor** [75% Primary Alignment] [██████████ 1/2] 6/8 Primary KK Items
 - **Primary Cognitive Levels:** Evaluate / Apply / Analyze
 - **M1 Core Topics:** Control effectiveness testing, ISO 19011/27007 auditing, 3 Lines of Defense, and conformity assessments.
- **Cybersecurity Architect** [73% Primary Alignment] [██████████ 1/2] 11/15 Primary KK Items
 - **Primary Cognitive Levels:** Create / Analyze / Evaluate
 - **M1 Core Topics:** Purdue Enterprise Model (Levels 0–5), MITRE DEFEND, zero-trust zones, and Privacy by Design.
- **Cybersecurity Implementer** [73% Primary Alignment] [██████████ 1/2] 8/11 Primary KK Items
 - **Primary Cognitive Levels:** Apply / Create / Analyze
 - **M1 Core Topics:** OS/network security baselines, firewall/EDR/SIEM installation, secure SDLC, and defensive scripting.
- **Digital Forensics Investigator** [69% Primary Alignment] [██████████ 1/2] 9/13 Primary KK Items
 - **Primary Cognitive Levels:** Analyze / Apply / Evaluate

- **M1 Core Topics:** Disk/memory forensics, malware analysis, OS/network event logs, and ISO 27037 chain of custody.
 - **Cyber Threat Intelligence (CTI) Specialist** [62% Primary Alignment] [██████████░░░░░░░░░░] 8/13 Primary KK Items
 - **Primary Cognitive Levels:** Analyze / Apply / Evaluate
 - **M1 Core Topics:** STIX/TAXII standards, MITRE ATT&CK/CAPEC mapping, threat actor profiling, and TTP analysis.
-

● Tier 3: Specialized Roles & Identified Curriculum Gaps

- **Cybersecurity Researcher** [80% Primary / 5 Total Items] [██████████░░░░░░░░░░] 4/5 Primary KK Items
 - **Primary Cognitive Levels:** Create / Evaluate / Analyze
 - **M1 Core Topics:** RDI, dual-use export rules, multidisciplinary synthesis, and vulnerability disclosure.
 - **Intended Curriculum Gap:** Lacks academic research publication frameworks.
- **Cybersecurity Educator** [25% Primary Alignment / 8 Total Items] [██████1/2░░░░░░░░░░] 2/8 Primary KK Items
 - **Primary Cognitive Levels:** Create / Evaluate / Apply
 - **M1 Core Topics:** Security awareness program development, habit reinforcement, and NIS2 training mandates.
 - **Intended Curriculum Gap:** Unaddressed formal pedagogical standards and educational *methodologies*.

(Analysis performed by NotebookLM based on the complete material, lectures, and case studies shared with and requested from Year 2026 participants.)