Automotive Cybersecurity Manager

The Automotive Cybersecurity Manager defines, implements, and oversees organisational cybersecurity strategies across the automotive product lifecycle. Main activities include setting up cybersecurity management systems, planning and auditing processes, ensuring regulatory compliance (UNECE R155/156, ISO/SAE 21434), and coordinating risk and incident management.

Responsibilities include aligning cybersecurity plans with corporate objectives, managing supplier security, coordinating audits, and providing evidence for homologation. The Manager collaborates with engineering, IT, operations, and external regulators to embed cybersecurity into both organisational and product domains.

Essential competences include digital (management systems, audits, incident response), sector-specific (homologation, ISO/SAE 21434, TARA), transversal (risk management, compliance, project management), soft competences (leadership, communication, analytical thinking), and other organisational competences (process planning, supplier security, governance).

ESCO Mapping

https://esco.ec.europa.eu/select-language?destination=/node/1

ID	NAME	Concept URI
2529.8	cybersecurity risk manager	http://data.europa.eu/esco/occupation/7754d570-9519-48c2-b1c9-8e165f8bca0f

Context

EQF Level	7
Departments	Production and Maintenance R&D (Research and Development)

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Digital Competences

ID	Name	Type	Description	Level	ESCO
C112	Cybersecurity management system	Knowledge	Organisational aspects of implementing a cybersecurity management system (CSMS). ▪ Describe CSMS elements ▪ Explain roles and responsibilities ▪ Monitor compliance with ISO/SAE 21434 ▪ Recommend improvements	2	
C113	Plan cybersecurity	Skill	Establish and monitor cybersecurity plans across the organisation. ▪ Define objectives and milestones ▪ Allocate resources ▪ Track progress and KPIs ▪ Align plans with business strategy	3	

Sector-Specific Competences

ID	Name	Type	Description	Level	ESCO
C289	Threat and risk analysis (TARA)	Knowledge	Methods for conducting threat and risk analyses. ▪ Explain asset analysis ▪ Identify attack targets ▪ Define cybersecurity goals ▪ Document results for projects	2	
C280	System design and vulnerability analysis	Knowledge	Methods for integrating security into automotive architectures. ▪ Explain secure design principles ▪ Recommend defensive patterns ▪ Review vulnerabilities in designs ▪ Support architecture reviews	2	
C290	Define cybersecurity software requirements	Knowledge	Requirements to secure critical automotive software. ▪ Identify critical functions ▪ Analyse risks to software ▪ Define requirements ▪ Document in specifications	2	
C282	Integrate cybersecurity	Knowledge	Principles for embedding cybersecurity in software design.	2	

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

ID	Name	Type	Description	Level	ESCO
	into software architecture		▪ Explain secure architecture concepts ▪ Define interface protections ▪ Align with ISO 21434 ▪ Review implementation		
C283	Secure software development	Knowledge	Guidelines and standards for secure software development. ▪ Explain MISRA/OWASP rules ▪ Describe secure coding practices ▪ Monitor vulnerabilities ▪ Recommend improvements	2	
C284	Cybersecure hardware and firmware design	Knowledge	Principles for integrating HSMs into ECU designs. ▪ Explain HSM functionality ▪ Describe secure firmware principles ▪ Support hardware/firmware security audits ▪ Document compliance evidence	2	
C285	Cybersecure software testing	Knowledge	Methods for testing secure coding and integration. ▪ Define test strategies ▪ Explain ISO 21434 testing guidance ▪ Review test evidence ▪ Identify vulnerabilities	2	
C286	Verify hardware security modules	Knowledge	Methods for verifying HSMs in automotive contexts. ▪ Explain HSM verification processes ▪ Document test evidence ▪ Support supplier reviews ▪ Monitor hardware compliance	2	
C287	Verify cybersecurity at system level	Knowledge	Methods for verifying cybersecurity across the vehicle/system. ▪ Define verification strategies ▪ Review EOL test evidence ▪ Support audits ▪ Identify gaps	2	
C288	Perform penetration testing	Skill	Plan and oversee penetration testing activities. ▪ Define scope of penetration tests ▪ Coordinate external experts ▪ Monitor vulnerabilities identified ▪ Review mitigation actions	2	

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Other Competences

ID	Name	Type	Description	Level	ESCO
C322	Legal and homologation aspects	Knowledge	Regulatory frameworks relevant to vehicle cybersecurity. ▪ Explain UNECE R155/156 ▪ Monitor homologation processes ▪ Identify compliance impacts Support teams during audits	2	
C323	Organisational structures	Knowledge	Structures required to manage cybersecurity governance. ▪ Describe governance frameworks ▪ Explain reporting lines ▪ Define stakeholder roles ▪ Support maturity assessments	2	
C325	Perform threat and vulnerability analysis	Skill	Oversee threat intelligence and vulnerability assessments across systems. ▪ Coordinate teams for asset identification ▪ Review results of TARAs ▪ Validate mitigation strategies Ensure updates to vulnerability databases	3	
C326	Manage cybersecurity processes and audits	Skill	Define, apply and review cybersecurity processes and audits. ▪ Establish audit scope ▪ Manage internal and external audits ▪ Review audit findings Ensure corrective actions are implemented	3	
C327	Manage incident response	Skill	Establish and coordinate organisational incident response procedures. ▪ Define incident response policies ▪ Coordinate cross-functional teams ▪ Report to authorities if required Review lessons learned	3	
C328	Manage supplier security	Skill	Define and monitor supplier cybersecurity requirements. ▪ Integrate requirements into contracts ▪ Conduct supplier audits ▪ Monitor DIAs and compliance reports Escalate risks to governance boards	3	

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.