















































































CompTIA Certifications and the NIS2				
	Decision Maker	IT Operations Team (ITOps)	Security Operations Team (SecOps)	Technical & Security Leadership
<p>This resource provides learners with a clear learning pathway by identifying the percentage of knowledge and skills alignment between CompTIA certifications and the roles defined in NIS2 (Network and Information Systems) Directive</p> <p>By presenting this alignment, learners can design their own customised learning journey while ensuring they meet the requirements outlined in NIS2.</p>	<ul style="list-style-type: none"> • Non-technical stakeholders who support organizational resilience. • Oversee and challenge IT and Security Operations teams on control implementation. • Non-Technical, but require understanding of key concepts to align business goals with technology resources. • Includes roles such as: <ul style="list-style-type: none"> • CEO / Managing Director • CFO / Finance Director • Security awareness leaders • Board members • Non-executive board members 	<ul style="list-style-type: none"> • Act as the first line of defence for network and information systems resilience • Operate within a broad and evolving technology landscape • Responsible for designing, implementing, securing, maintaining, and supporting tech infrastructure • Includes IT roles such as: <ul style="list-style-type: none"> • IT Support Technicians • Systems and Network Administrators • Network and Cloud Engineers • Database Administrators 	<ul style="list-style-type: none"> • Security Operations may be a separate team or part of IT Operations • Focuses on managing, monitoring, testing, and reporting on cyber security resilience • Includes roles such as: <ul style="list-style-type: none"> • Security Administrators • Cyber Security Analysts • Penetration Testers 	<ul style="list-style-type: none"> • Responsible for: <ul style="list-style-type: none"> • Implementing and reporting on NIS2 directive • Ensuring continuous improvement of security posture • Horizon scanning for emerging cybersecurity opportunities and threats • Includes leaders overseeing IT and Security Operations, such as: <ul style="list-style-type: none"> • CTO, CISO • Team leaders, managers, and directors

NIS2 Minimum Measures & Linkages to CompTIA Solutions

NIS2 Minimum Measure		Decision Maker (nontechnical)	IT Operations Team (ITOps)	Security Operations Team (SecOps)	Technical & Security Leadership
1	Risk assessments and security policies for information systems.		  		 
2	A plan for handling security incidents.		  	 	 
3	A plan for managing business operations during and after a security incident. This means that backups must be up to date. There must also be a plan for ensuring access to IT systems and their operating functions during and after a security incident.		     	 	 

4	Security around supply chains and the relationship between the company and direct supplier. Companies must choose security measures that fit the vulnerabilities of each direct supplier. And then companies must assess the overall security level for all suppliers.			 	 
5	Policies and procedures for evaluating the effectiveness of security measures.		 	 	
6	Security around the procurement of systems and the development and operation of systems. This means having policies for handling and reporting vulnerabilities.			 	 
7	Cybersecurity training and a practice for basic computer hygiene.		   	 	 

			 		
8	Policies and procedures for the use of cryptography and, when relevant, encryption.		     		 
9	Security procedures for employees with access to sensitive or important data, including policies for data access. The company must also have an overview of all relevant assets and ensure that they are properly utilized and handled.		     	 	

10	The use of multi-factor authentication, continuous authentication solutions, voice, video, and text encryption, and encrypted internal emergency communication, when appropriate.		    	 	 
----	---	--	---	---	---