CompTIA Certifications and DORA Regulations	**Decision Maker**	**IT Operations Team (ITOps)**	**Security Operations Team (SecOps)**	**Technical & Security Leadership**
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 the DORA (Digital Operation Resilience Act) Regulations By presenting this alignment, learners can design their own customised learning journey while ensuring they meet the requirements outlined in DORA.	• Oversee and challenge IT and Security Operations to ensure appropriate controls • Support strategic decisions in: • ICT risk management • Digital resilience testing • Third-party service oversight • Require understanding of key concepts to balance business goals with technology investments • Includes non-technical stakeholders: • CEO/Managing Director • CFO/Finance Director • Security awareness leaders, board members, and non-executive directors	• Responsible for designing, implementing, securing, and maintaining the technology landscape • Serve as the first line of defence for digital operational resilience • Support compliance with DORA requirements: • Robust ICT risk management • Systems continuity • Includes roles such as: • IT Support Technicians • Systems and Network Administrators • Network and Cloud Engineers • Database Administrators	• May be a distinct function or part of the IT Operations Team • Members have defined cybersecurity and resilience responsibilities • Key functions include: • Managing, monitoring, testing, and reporting on cybersecurity resilience • Responding to incidents • Conducting resilience exercises (as required by DORA) • Includes roles such as: • Security Administrators • Cyber Security Analysts • Penetration Testers	• Accountable for DORA implementation and reporting obligations • Drive continuous improvement in digital operational resilience • Coordinate with third-party suppliers • Monitor emerging digital risks and regulatory changes • Includes senior leaders such as: • Chief Technology Officer (CTO) • Chief Information Security Officer (CISO) • Team leads, managers, and directors

DORA – 5 Pillars & Linkages to CompTIA Solutions

Pillar 1, ICT Risk Management

Article Number	DORA Measures	Decision Maker (nontechnical)	IT Operations Team (ITOps)	Security Operations Team (SecOps)	Technical & Security Leadership
Article 4	Governance & Management Accountability Management and board responsibility for ICT risk, strategy, policies, resources, and oversight.	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
Article 5	ICT Risk Management Framework Holistic risk management: identification, protection, detection, recovery, reviews.	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA Server+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series CompTIA PenTest+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
Articles 6-8	Asset, Configuration & Change Management Asset inventory, secure configurations, formal change control.	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA Server+ CERTIFICATION Plus Series CompTIA Data+ CERTIFICATION Plus Series CompTIA DataSys+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series

Articles 9-10	Data Integrity, Availability, and Backup/Restoration Data protection, routine backups, restoration planning/testing.	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA Server+ CERTIFICATION Plus Series CompTIA Data+ CERTIFICATION Plus Series CompTIA DataSys+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
Article 11	Secure Software Development Secure coding/SDLC, reviews at all stages, tracked vulnerabilities.	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA Linux+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA PenTest+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
Article 12	ICT Change and Patch Management Formal processes for patches/changes, logging, risk checks, fast fixes.	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA Linux+ CERTIFICATION Plus Series CompTIA Server+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
Article 13	ICT Security & Awareness Training Regular security training for all, role-based detail, specialist training.	CompTIA Tech+ CERTIFICATION Plus Series CompTIA Project+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series

Article 14	ICT Operations, Maintenance, Monitoring Robust daily ops, continuous monitoring, maintenance, incident log review.	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA DataSys+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
Article 15	Physical & Environmental Security Restrict access, protect ICT from physical/environmental threats.	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Server+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
Article 16	Communications Security Encrypt data in transit, secure comms (internal, external), monitoring.	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA Network+ CERTIFICATION Plus Series CompTIA Linux+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA Data+ CERTIFICATION Plus Series CompTIA DataSys+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series

CompTIA.

Pillar 2, ICT Incident Management

Article Number	DORA Measures	Decision Maker (nontechnical)	IT Operations Team (ITOps)	Security Operations Team (SecOps)	Technical & Security Leadership
Article 17	ICT Related Incident Management Define and use procedures to detect, assess, manage, and document ICT incidents that impact operations.	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA Server+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
Article 18	Classification of ICT Related Incidents Classify incidents by severity and impact, to ensure correct prioritisation and escalation	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA Server+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
Article 19	Major ICT Related Incident Notification Notify regulators swiftly when incidents meet the 'major' threshold according to established criteria.	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA Server+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series

Article 20	Reporting of ICT Related Incidents to Authorities Provide full, timely incident reports to authorities, following regulatory guidelines	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA Server+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
Article 21	Follow-Up Reports Submit lessons learned, closure, and improvement reports after resolving issues	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA Server+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series CompTIA PenTest+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
Article 22	Significant Cyber Threat Reporting Report emerging or significant cyber threats to authorities to benefit the wider sector	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA Server+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
Article 23	Voluntary Incident Reporting Report additional incidents voluntarily to enhance sector resilience and intelligence	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA Server+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series

Pillar 3, Digital Operational Resilience Testing

Article Number	DORA Measures	Decision Maker (nontechnical)	IT Operations Team (ITOps)	Security Operations Team (SecOps)	Technical & Security Leadership
Article 24	General Testing Framework Implement a formal, risk-based strategy for regular testing of ICT systems, proportionate to the organisation's size, business, and risk exposure.	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA Server+ CERTIFICATION Plus Series CompTIA Linux+ CERTIFICATION Plus Series CompTIA DataSys+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series CompTIA PenTest+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
Article 25	Advanced Testing Conduct advanced resilience testing (e.g. threat-led penetration tests) for critical systems and functions, including simulated attacks mirroring real cyber threats.	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA Server+ CERTIFICATION Plus Series CompTIA Linux+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA PenTest+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series

Article 26	Ongoing Programme Review and Adaptation Routinely review and adapt the organisation’s testing programme in response to evolving threats, technologies, and business processes.	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA Server+ CERTIFICATION Plus Series CompTIA Linux+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series CompTIA PenTest+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series

Pillar 4, ICT Third Party Risk Management

Article Number	DORA Measures	Decision Maker (nontechnical)	IT Operations Team (ITOps)	Security Operations Team (SecOps)	Technical & Security Leadership
Articles 28-31	Third Party Due Dilligence and Risk Assessment Assess ICT suppliers before engagement, considering their resilience, security practices, service levels, and regulatory risks.	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA DataSys+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
Articles 32-34	Contract Management, Registers, and Oversight Ensure contracts include clear security, audit, service and exit requirements; maintain a register of ICT suppliers and arrangements.	CompTIA Tech+ CERTIFICATION Plus Series		CompTIA Security+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
Articles 35-38	Ongoing Oversight, Monitoring and Exit Plans Regularly monitor suppliers for compliance and emerging risk; have documented, tested exit and transition plans.	CompTIA Tech+ CERTIFICATION Plus Series			CompTIA SecurityX CERTIFICATION Xpert Series

Articles 39-44	Concentration and Sub-Outsourcing Risk Identify and mitigate risk from supplier concentration and sub-suppliers; avoid excessive dependency on a single provider.	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA DataSys+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
Articles 46-57	Oversight of Critical Third Parties Critical ICT providers (e.g., major cloud or infrastructure services) are subject to EU-level supervisory oversight, direct audits, and enforcement actions.	CompTIA Tech+ CERTIFICATION Plus Series			CompTIA SecurityX CERTIFICATION Xpert Series

Pillar 5, Information Sharing Arrangements

Article Number	DORA Measures	Decision Maker (nontechnical)	IT Operations Team (ITOps)	Security Operations Team (SecOps)	Technical & Security Leadership
Article 45	Information Sharing Arrangements Encourage voluntary participation in trusted information-sharing groups to exchange cyber threat intelligence, incidents, vulnerabilities, and mitigation techniques, always in compliance with data protection and confidentiality rules.	CompTIA Tech+ CERTIFICATION Plus Series	CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series