CompTIA Certifications and the Cyber Resilience Act (CRA)	**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 Cyber Resilience Act (CRA) By presenting this alignment, learners can design their own customised learning journey while ensuring they meet the requirements outlined in the CRA.	• Contribute to resilience by overseeing and challenging IT and Security Operations • Must understand key concepts to align business goals with tech investments • Support strategic decisions in areas like: • Security by design • Vulnerability and incident management • Third-party product oversight • Non-technical stakeholders such as: • CEO, Finance Director • Security awareness leaders • Board members, non-executive directors	• Responsible for designing, implementing, securing, and maintaining the organisation's technology environment • Acts as the first line of defence for digital resilience • Supports compliance with CRA requirements: • Secure configurations • Timely security updates • Robust system maintenance • Includes roles such as: • IT Support Technicians • Systems and Network Administrators • Network and Cloud Engineers • Database Administrators	• May be a dedicated function or part of the IT Operations Team • Team members have specific cybersecurity responsibilities • Key functions include: • Managing, monitoring, testing, and reporting on cyber resilience • Responding to security incidents • Overseeing vulnerability management • Leading security incident reporting and disclosure (as required by CRA) • Includes roles such as: • Security Administrators • Cyber Security Analysts • Penetration Testers	• Accountable for CRA implementation and compliance • Drive continuous improvement in cyber resilience • Coordinate with third-party suppliers • Monitor emerging cyber risks and regulatory changes • Includes roles such as: • Chief Technology Officer (CTO) • Chief Information Security Officer (CISO) • Team leads, managers, and directors

© 2025 CompTIA, Inc., used under license by CompTIA, Inc. All rights reserved.
All certification programs and education related to such programs are operated exclusively by CompTIA, Inc.
CompTIA is a registered trademark of CompTIA, Inc. in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA, Inc. or of their respective owners.
Reproduction or dissemination prohibited without the written consent of CompTIA, Inc. 11734 Printed in the US 082025

CRA Key Scope Areas & Linkages to CompTIA Solutions

CRA Requirements		Decision Maker (nontechnical)	IT Operations Team (ITOps)	Security Operations Team (SecOps)	Technical & Security Leadership
1	Security by Design and by Default All digital products must be developed with cybersecurity built in from the outset, and should be delivered with secure settings as standard.		CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
2	Vulnerability Management and Disclosure Manufacturers must establish clear, ongoing processes for receiving, addressing, and communicating about security vulnerabilities throughout the product lifecycle.		CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series CompTIA PenTest+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
3	Timely Security Updates and Patch Management Products must support rapid, secure delivery of patches and updates to fix vulnerabilities and maintain protection.		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 DataSys+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series

© 2025 CompTIA, Inc., used under license by CompTIA, Inc. All rights reserved.
All certification programs and education related to such programs are operated exclusively by CompTIA, Inc.
CompTIA is a registered trademark of CompTIA, Inc. in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA, Inc. or of their respective owners.
Reproduction or dissemination prohibited without the written consent of CompTIA, Inc. 11734 Printed in the US 082025

4	Conformity Assessment and CE Marking Products must be assessed—by the manufacturer or an independent body—for cybersecurity compliance before being sold in the EU, and CE marking must be displayed.			CompTIA Security+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
5	Technical Documentation and Record-Keeping Comprehensive documentation on cybersecurity measures, risk assessments, software/firmware versions, and incident handling must be kept up to date and made available for inspection.		CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series CompTIA Server+ CERTIFICATION Plus Series CompTIA DataSys+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
6	Transparent User Instructions and Security Information Users must be given straightforward guidance on using product security features, installing updates, and following best practices to stay protected.			CompTIA Security+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series

© 2025 CompTIA, Inc., used under license by CompTIA, Inc. All rights reserved.
All certification programs and education related to such programs are operated exclusively by CompTIA, Inc.
CompTIA is a registered trademark of CompTIA, Inc. in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA, Inc. or of their respective owners.
Reproduction or dissemination prohibited without the written consent of CompTIA, Inc. 11734 Printed in the US 082025

7	Incident and Vulnerability Reporting Organisations must notify relevant authorities (and sometimes users) of serious security incidents and actively exploited vulnerabilities within strict deadlines (e.g., 24 hours).		CompTIA A+ CERTIFICATION Plus Series CompTIA Network+ CERTIFICATION Plus Series CompTIA Cloud+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series CompTIA CySA+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
8	Lifecycle Security Maintenance Manufacturers must provide continued security support—including updates, fixes, and vulnerability management—throughout the declared support period for the product.		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 SecurityX CERTIFICATION Xpert Series
9	Critical Product Third-Party Assessment Products deemed highly critical (e.g., security software, some network devices) require independent cybersecurity assessments beyond self-evaluation.			CompTIA Security+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series
10	Supply Chain and Third-Party Security Manufacturers must ensure integrated components (including open-source and third-party software) also meet CRA security standards, and maintain supply chain transparency.		CompTIA DataSys+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series

© 2025 CompTIA, Inc., used under license by CompTIA, Inc. All rights reserved.
All certification programs and education related to such programs are operated exclusively by CompTIA, Inc.
CompTIA is a registered trademark of CompTIA, Inc. in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA, Inc. or of their respective owners.
Reproduction or dissemination prohibited without the written consent of CompTIA, Inc. 11734 Printed in the US 082025

11	Market Surveillance and Enforcement Organisations must cooperate with regulators, support product recalls if required, and be prepared for market checks or enforcement actions relating to non-compliance.		CompTIA Network+ CERTIFICATION Plus Series	CompTIA Security+ CERTIFICATION Plus Series	CompTIA SecurityX CERTIFICATION Xpert Series

© 2025 CompTIA, Inc., used under license by CompTIA, Inc. All rights reserved.
All certification programs and education related to such programs are operated exclusively by CompTIA, Inc.
CompTIA is a registered trademark of CompTIA, Inc. in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA, Inc. or of their respective owners.
Reproduction or dissemination prohibited without the written consent of CompTIA, Inc. 11734 Printed in the US 082025