Table of contents

Detailed agenda of the training course

Day 1 Introduction to the concepts and requirements of DORA

Standards cited in this training course

- ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks
- ISO 55000:2014. Asset management — Overview, principles and terminology
- ISO 22300:2021, Security and resilience — Vocabulary

- ISO 31000:2018, Risk management — Guidelines
- ISO 31010:2019, Risk management — Risk assessment techniques
- ISO 31073:2022, Risk management — Vocabulary
- ISO 37301:2021, Compliance management systems — Requirements with guidance for use
- ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements
- ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301
- ISO 22316:2017, Security and resilience — Organizational resilience — Principles and attributes
- ISO 22361:2022, Security and resilience — Crisis management — Guidelines for a strategic capability
- ISO/IEC 27031:2011, Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 27035-2:2023, Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response
- ISO/IEC 27035-1:2023, Information technology — Information security incident management — Part 1: Principles and process
- NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment
- ISO 10015:2019, Quality management — Guidelines for competence management and people development

Bibliography

Section 2: Overview of the Digital Operational Resilience Act (DORA)

[1] Deloitte. "Exploring DORA." *Deloitte*. Accessed February 5, 2024. https://www2.deloitte.com/lu/en/pages/risk/articles/exploring-dora.html

[2] Heuking. "Digitial Operational Resilience Act and Cyber Resilience Act: New EU Requirements for Cybersecurity." *Heuking.* Last modified February 13, 2023. https://www.heuking.de/en/news-events/newsletter-articles/detail/digital-operational-resilience-act-and-cyber-resilience-act-new-eu-requirements-for-cybersecurity.html

Section 3: Fundamental concepts of ICT risk management and digital operational resilience

[1] European Banking Authority. EBA Guidelines on ICT and Security Risk Management. November 29, 2019. https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf

[2] Mardsen, Erik. "The ISO 31000 Standard on Risk Management." *Risk Engineering*. Accessed March 6, 2024. https://risk-engineering.org/static/PDF/slides-ISO31000-risk-management.pdf

[3] IBM. "What Is Risk Management?" Accessed February 5, 2024. https://www.ibm.com/topics/risk-management

[4] M Studio. "Residual Risk." Last modified December 23, 2011. https://riskmanagementstudio.com/wp-content/uploads/2011/04/RM_Studio_Residual_Risk.pdf

[5] Klidow, A. Betty. *A Supply Chain Management Guide to Business Continuity*. New York: AMACOM, 2011. (p. 257)

[6] Denyer, David. *Organizational Resilience: A summary of academic evidence, business insights and new thinking.* Cranfield: BSI and Cranfield University, 2017. (p. 5)

[7] Leflar, J. James, and Marc H. Siegel. *Organizational Resilience: Managing the Risks of Disruptive Events — A Practitioner's Guide.* New York: CRC Press, 2013. (p. 12)

[8] RiskOptics. "What Is Digital Resilience?" Last modified August 19, 2022. https://reciprocity.com/resources/what-is-digital-resilience/

[9] CISCO. "What Is Cyber Resilience?" Accessed February 5, 2024. https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-cyber-resilience.html

[10] Dataminr. "Business Continuity vs. Business Resilience." https://www.dataminr.com/resources/business-continuity-vs-business-resilience.

[11] Villegas, Fabyio. "Organizational Resilience: What It Is & How to Build It." QuestionPro, May 4, 2023. https://www.questionpro.com/blog/organizational-resilience/.

[12] Capodagli, Stefano. "Digital Risk Management and Resiliency." *Enterprise Risk*. Last modified January 18, 2019. https://enterpriseriskmag.com/2019/01/digital-risk-management-and-resiliency-part-one/#:~:text=Building%20digital%20resiliency%20both%20in%20terms%20of%20strategy,mitigate%20and%20minimise%20financial%20losses%20and%20business%20disruption

Section 4: Preparing and planning for DORA project implementation

[1] WallStreetPrep. "Step-by-step Guide to Understanding Stakeholders in Corporate Finance." Last modified May 5, 2023. https://www.wallstreetprep.com/knowledge/stakeholders/

[2] Pirrozi, Massimo. Effectively managing negative and natural stakeholders. PMWorld Journal. Accessed April 15, 2024. https://pmworldjournal.com/article/effectively-managing-negative-and-neutral-stakeholders

[3] Post, James E., Anne T. Lawrence, and James Weber. *Business and Society: Corporate Strategy, Public Policy and Ethics.* McGraw-Hill/Irwin, 2002.

[4] Whittington, Richard, Patrick Regnér, Duncan Angwin, Gerry Johnson, and Kevan Scholes. *Exploring Strategy — Text and Cases.* 12th edition. Harlow: Pearson Education Limited, 2020.

[5] CFI Team. "Corporate Structure." *Corporate Finance Institute.* Accessed February 14, 2024. https://corporatefinanceinstitute.com/resources/accounting/corporate-structure/

[6] Kelleher, Shane. "DORA: Management of ICT Third-party Risk." *William Fry*. Last modified May, 2023. https://www.williamfry.com/knowledge/dora-management-of-ict-third-party-risk

[7] Blizzard, Keith. "How to Prepare for the Digital Operational Resilience Act (DORA)." Johnson Hana. Last modified August 9, 2023. https://www.johnsonhana.com/how-to-prepare-for-the-digital-operational-resilience-act-dora/

Section 5: Governance and organization

[1] Anderson, Douglas J. and Gina Eubanks. *Leveraging COSO across the Three Lines of Defense*. The Institute of Internal Auditors, 2015. https://riskcue.id/uploads/ebook/20211013105542-2021-10-13ebook105459.pdf

[2] CIPS Knowledge. "Monitoring the Performance of Suppliers." *CIPS Knowledge.* Accessed February 6, 2024. https://www.cips.org/documents/knowledge/procurement-topics-and-skills/9-supplier-bid-tender-evaluation/supplier-evaluation-and-appraisal/pop-monitoring_the_performance_of_suppliers.pdf

Section 6: ICT risk management

[1] James, Priya. "10 Best Vulnerability Scanner Tools For Penetration Testing – 2023." *GBHackers on Security.* Accessed February 12, 2024. https://gbhackers.com/vulnerability-scanner-tools/amp/

[2] "Security Test and Evaluation (ST&E)." *NIST*. Accessed February 12, 2024. https://csrc.nist.gov/glossary/term/security_test_and_evaluation
[3] "Penetration Testing." *FORTA*. Accessed February 12, 2024. https://www.coresecurity.com/penetration-testing
[4] Bacchelli, Alberto, and Christian Bird. "Expectations, Outcomes, and Challenges of Modern Code Review." In *2013 35th International Conference on Software Engineering (ICSE)*, pp. 712-721. IEEE, 2013. https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/ICSE202013-codereview.pdf
[5] "ERM Risk Owner – Roles and Responsibilities?" *University of Oregon*. Accessed January 18, 2023. https://safety.uoregon.edu/erm-risk-owner-roles-and-responsibilities
[6] European Union Agency for Cybersecurity. "Risk Assessment." Accessed February 8, 2024. https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-process/risk-assessment
[7] Fraser, John R.S., Betty J. Simkins, and Kristina Narvaez, eds. *Implementing Enterprise Risk Management: Case Studies and Best Practices*. New Jersey: John Wiley & Sons, Inc., 2015.
[8] New Zealand Government. "ICT Risk Management Guidance." New Zealand Government. Last modified December 3, 2020. https://www.digital.govt.nz/dmsdocument/130-ict-risk-management-guidance/html
[9] Jhanjhi, Noor Zaman, Khalid Hussain, Azween Bin Abdullah, Mamoona Humayun, and João Manuel R.S. Tavares. *Information Security Handbook.* Boca Raton: CRC Press, 2022.
[10] Fennelly, Lawrence J., and Marianna A. Perry. *Physical Security: 150 Things You Should Know*. Cambridge: Elsevier, 2017. https://www.sciencedirect.com/topics/computer-science/risk-avoidance
[11] "Approve a Risk Quick Reference Guide." *James Cook University*. December 01, 2022. https://www.jcu.edu.au/__data/assets/pdf_file/0009/1947762/RiskWare-QR-Guide-Approve-a-Risk.pdf
[12] Gerken, Nils Hoffmann, Andreas Kremer. "Getting risk ownership right." *McKinsey&Company*. November 2010. https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/working%20papers/23_getting_risk_ownership_right.ashx
[13] Popov, Georgi, Bruce K. Lyon, and Bruce Hollcroft. *Risk Assessment: A Practical Guide to Assessing Operational Risks.* New Jersey: John Wiley & Sons Inc., 2016.
[14] ServiceNow. "What Is IT Change Management?" Accessed February 13, 2024. https://www.servicenow.com/products/itsm/what-is-it-change-management.html
[15] The Institute of Internal Auditors. "IT Change Management: Critical for Organizational Success." (2021): 9. Accessed February 13, 2024. https://iia.no/wp-content/uploads/2020/02/2020-GTAG-IT-Change-Management.pdf
[16] Hyperproof. "Segregation of Duties: What It Is and Why It's Important." Last modified February 3, 2022. https://hyperproof.io/resource/segregation-of-duties/

[17] The Institute of Internal Auditors. "IT Change Management: Critical for Organizational Success." (2021): 10. Accessed February 13, 2024. https://iia.no/wp-content/uploads/2020/02/2020-GTAG-IT-Change-Management.pdf
[18] ManageEngine. "10 ITIL Change Management Best Practices for an Organization" *ManageEngine*. Accessed February 13, 2024. https://www.manageengine.com/products/service-desk/itil-change-management/itil-change-management-best-practices.html#best-practices
[19] Rock, Tracy. "9 Critical Business Continuity Plan Objectives." *Invenio IT*. Last modified March 5, 2022. https://invenioit.com/continuity/business-continuity-plan-objectives/
[20] Kosutic, Dejan. "Business Continuity Plan: How to Structure It According to ISO 22301." *Advisera*. Accessed February 12, 2024. https://advisera.com/27001academy/knowledgebase/business-continuity-plan-how-to-structure-it-according-to-iso-22301/
[21] *IBM*. "What Is a Disaster Recovery (DR) Plan." Accessed February 12, 2024. https://www.ibm.com/topics/disaster-recovery-plan
[22] Cloudian. "IT Disaster Recovery Plan." Accessed February, 8, 2024. https://cloudian.com/guides/disaster-recovery/it-disaster-recovery-plan/#
[23] Wallace, Michael, and Lawrence Webber. *The Disaster Recovery Handbook*. New York: AMACOM, 2018.

[24] Institute for Public Relations. "Crisis Management and Communications." Last modified October 30, 2007. https://instituteforpr.org/crisis-management-and-communications/#:~:text=Crisis%20management%20can%20be%20divided,actually%20respond%20to%20a%20crisis

Section 7: ICT-related incident management and reporting

[1] ComplianceQuest. "The Lifecycle of Incident Management: Purpose, Process and Resolution Plan." Accessed February 8, 2024. https://www.compliancequest.com/incident-management/
[2] Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. "Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology." *NIST*, rev.2 (2012): 25-34. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Section 8: Digital operational resilience testing

[1] "What is vulnerability assessment? Benefits, tools, and process." Hackerone. Accessed February 8, 2024. https://www.hackerone.com/knowledge-center/what-vulnerability-assessment-benefits-tools-and-process
[2] Mwendia, Dickson. "Open Source Analysis Checklist." Medium. Last modified May 15, 2020. https://medium.com/@Dickson_Mwendia/open-source-analysis-checklist-3a9dc2b25cc8
[3] Rosen, Jj. "Network security assessments: Importance and Best Practices." Atiba. Last modified October 5, 2023. https://www.atiba.com/network-security-assessment/
[4] "Physical security review." Canaudit. Accessed February 8. 2024. https://www.canaudit.com/our-services/it-security-and-it-audit-services/physical-security-review
[5] Stancu, Livia. "29 Great Survey Software and Questionnaire Tools for 2023." Hubspot. Last modified October 16, 2023. https://blog.hubspot.com/service/survey-software
[6] "What is a code review?" Gitlab. Accessed February 8, 2024. https://about.gitlab.com/topics/version-control/what-is-code-review/
[7] "Scenario Testing – Software Testing." Geeksforgeeks. Last modified December 27, 2023. https://www.geeksforgeeks.org/software-testing-scenario-testing/
[8] Chatterjee, Shormistha. "What is Compatibility Testing?" Browerstack. Last modified August 6, 2023. https://www.browserstack.com/guide/compatibility-testing
[9] "Performance Testing." Geeksforgeeks. Last modified November 28, 2023. https://www.geeksforgeeks.org/performance-testing-software-testing/
[10] "What is end-to-end testing?" Screenster. Last modified September 25, 2018. https://www.screenster.io/end-to-end-testing/
[11] "What is penetration testing?" IBM. Accessed February 8, 2024. https://www.ibm.com/topics/penetration-testing
[12] Hackerone. "What Is Vulnerability Assessment? Benefits, Tools, and Process". Accessed May 8, 2023 https://www.hackerone.com/knowledge-center/what-vulnerability-assessment-benefits-tools-and-process
[13] "Vulnerability Scanners and Scanning Tools: What To Know." *Balbix*. Accessed February 12, 2024. https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/
[14] GFMA. A Framework for Threat-Led Penetration Testing in the Financial Services Industry. December 2, 2020. https://www.gfma.org/wp-content/uploads/2020/12/gfma-penetration-testing-guidance-for-regulators-and-financial-firms-version-2-december-2020.pdf

Section 9: Managing ICT third-party risks

[1] IPPF. "Auditing Third-party Risk Management." The Institute of Internal Auditors. October, 2018. https://iia.no/wp-content/uploads/2019/10/2018-PG-Auditing-third-party-Risk-Management.pdf

[2] "Enhancing Third-party Risk Management and Oversight." Financial stability board. June 22, 2023. https://www.fsb.org/wp-content/uploads/P220623.pdf

Section 11: Information and intelligence sharing

[1] "What is threat intelligence?" IBM. Accessed February 15, 2024. https://www.ibm.com/topics/threat-intelligence
[2] "Information Sharing Best Practices." H-ISAC. 2020. https://h-isac.org/wp-content/uploads/2020/03/H-ISAC-Information-Sharing-Best-Practices-March-2020.pdf
[3] "Information Sharing Best Practices." H-ISAC. 2020. https://h-isac.org/wp-content/uploads/2020/03/H-ISAC-Information-Sharing-Best-Practices-March-2020.pdf
[4] Acora One. "Cyber Security Awareness Tips For Employees." Last modified July 4, 2023. https://acora.one/news/article/cyber-security-awareness-tips-for-employees
[5] "Data sharing in financial services: Five techniques to enhance privacy and confidentiality." Deloitte. 2019. https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/gx-fsi-executive-summary-data-sharing-2019.pdf

Section 12: Training and awareness

[1] Cybersecurity and Infrastructure Security Agency. *CRR Supplemental Resource Guide: Training and Awareness.* Carnegie Mellon University. 2016. https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-TA_0.pdf
[2] INC. Training and Development. (n.d.). Accessed March 29, 2023. https://www.inc.com/encyclopedia/training-and-development.html
[3] Verma, Eshna. "How to Measure Training Effectiveness in 2024." Simplilearn. Last modified February 7, 2024. https://www.simplilearn.com/how-to-measure-effectiveness-corporate-training-article

Section 14: Internal audit and management review

[1] ECIIA. "DORA: The Digital Operational Resilience Act and Its Impact in the Financial Services." Last modified October 18, 2023. https://iia.no/wp-content/uploads/2023/10/2023-DORA-3.pdf (p. 5)
[2] Brun, Jonathan. "Maximizing Your Compliance Audit: A Practical Approach to Conducting Effective Internal Audits." *Nimonik Inc.* Last modified May 9, 2023. https://nimonik.com/2023/05/maximizing-your-compliance-audit-a-practical-approach-to-conducting-effective-internal-audits/

List of acronyms

BCP: Business Continuity Plan
BCMS: Business Continuity Management System
CMP: Crisis Management Plan
CRA: Cyber Resilience Act
CRM: Customer Relationship Management
CSIRT: Computer Security Incident Response Team
DORA: Digital Operational Resilience Act
DRP: Disaster Recovery Plan
EBA: European Banking Authority
EIOPA: European Insurance and Occupational Pensions Authority
ENISA: The European Union Agency for Cybersecurity
ESA: European Supervisory Authorities
ESMA: European Securities and Markets Authority
FTP: File Transfer Protocol
HE: Homomorphic Encryption
ICT: Information and Communication Technology
IMT: Incident Management Team
IRT: Incident Response Team
IT: Information Technology
JON: Joint Oversight Network
KPIs: Key Performance Indicators
MAD: Maximum Acceptable Downtime
OSA: Open-source Analyses
OSSTMM: Open Source Security Testing Methodology Manual
PECB: Professional Evaluation and Certification Board
PET: Privacy Enhancing Techniques
PII: Personally identifiable information
PoC: Point of Contact
ROE: Rules of Engagement
RPO: Recovery Point Objective
RTO: Recovery Time Objective
RTS: Regulatory Technical Standards
SLAs: Service-level Agreements
SMC: Secure Multiparty Computation
SoA: Statement of Applicability
SQL: Structures Query Language
STE: Security Testing and Evaluation
TLPT: Threat-led Penetration Testing

TTPs: Tactics, Techniques, and Procedures
ZKP: Zero-knowledge Proofs