Collaborative Cyber & Quality Assurance Learning: Meeting Compliance Through Integrated Paths

Testing Assembly 20.11.2025, Helsinki Finland

Mikko Paloheimo & Michael Peltonen, OP Financial Group

Speaker Bio

Mikko Paloheimo

Expert QA Lead & Chapter Lead,
Headmaster OP Tech Academy

OP Financial Group, Finland

Quality Assurance, Learning and
Development + QA Community...
what else is there?

Speaker Bio

Michael Peltonen

Cyber Security Expert

OP Financial Group, Finland

Cyber Security, Learning and Development. Passionate about securing digital services.

Context –
OP Financial Group from testers perspective

- Industries:
  - Retail & Corporate Banking and Insurance
    + a load of technology to run it all
- Employees:
  - 14000+ in the whole OP Financial Group
  - 4500 In Development & Technologies
  - 370 test engineers
  - 100 cyber security specialists
- Service scope:
  - Approx 1000 applications & services being run and developed
- Test automation scope:
  - Approx 6 million automated test cases running monthly

OP Tech Academy Overview and Learning Towers

OP Financial Group's One-stop shop for strategic technology competence development.

Platform for professional development

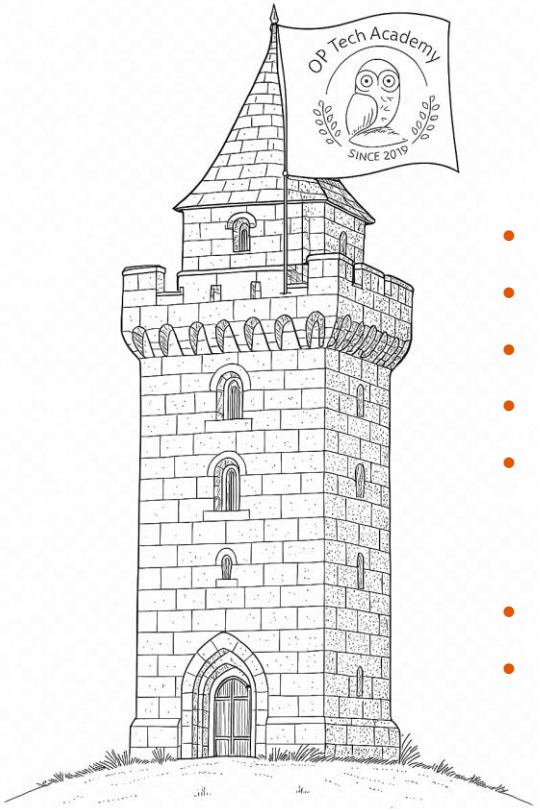
7 learning paths (towers) with courses for different skills levels

Specialists acts as mentors to support learning

Open to all employees

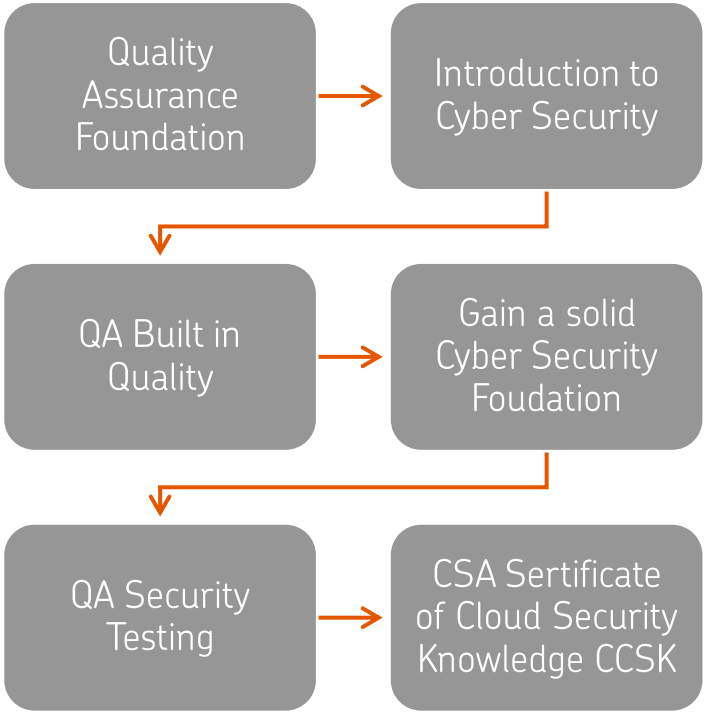
Spring and
Autumn semesters & selfstudy courses

Great way to use the 10 in OP Financial Group's 70-20-10 model!



- AI
- Data
- Development
- DevOps
- Designing and Leading Value Creation
- Quality Assurance
- Security

Tailored Learning Paths for Continuous Development



- **Personalized Adaptive Learning**
  - Adaptive strategies tailor content to individual roles, increasing relevance and engagement.
- **Structured Learning Journeys**
  - Employees progress from foundational to advanced courses, ensuring solid knowledge before specialization.
- **Diverse Learning Techniques**
  - Integration of self-paced modules, hands-on practice, and peer collaboration supports varied learning styles.
- **Mentorship and Real Projects**
  - Mentorship and real-world projects enhance professional growth and continuous improvement culture.

Quality Assurance and Security: Bridging Knowledge Areas

- Common goals. Both QA and security aim to reduce risk, ensure compliance, and protect customer trust:
  - QA ensures that bugs, defects, and usability issues are caught early.
  - Cyber Security ensures that vulnerabilities, misconfigurations, and attack vectors are identified and mitigated.

- Collaboration opportunities. In the Software Development Life-cycle (SDLC) there are plentiful of opportunities for collaboration:
  - Joint Requirements Review:
    - QA and Cyber Security teams review business and technical requirements together.
  - Threat Modeling & Test Planning:
    - Security experts contribute threat scenarios; QA incorporates them into test cases.
  - Integrated Testing:
    - QA conducts functional, performance, and usability tests.
    - Cyber Security performs vulnerability scans, penetration tests, and static code analysis.
  - Shared Tools: Use platforms like Jira, Confluence, or Azure DevOps to track issues and document findings.

Collaborative Learning Initiatives: Strengthening Compliance

- Interdisciplinary Learning Approach
  - QA and Security specialists collaborate to build shared compliance understanding and methodologies from the start.
- Critical Training Modules
  - Training covers risk management, scenario-based testing, and regulatory frameworks to navigate complex compliance.
- Successful Collaboration Benefits
  - Joint efforts enable early risk detection, streamlined audits, and reduce duplicated work.
- Proactive Compliance Culture
  - Embedding compliance in daily operations strengthens resilience and prepares teams for future regulations.

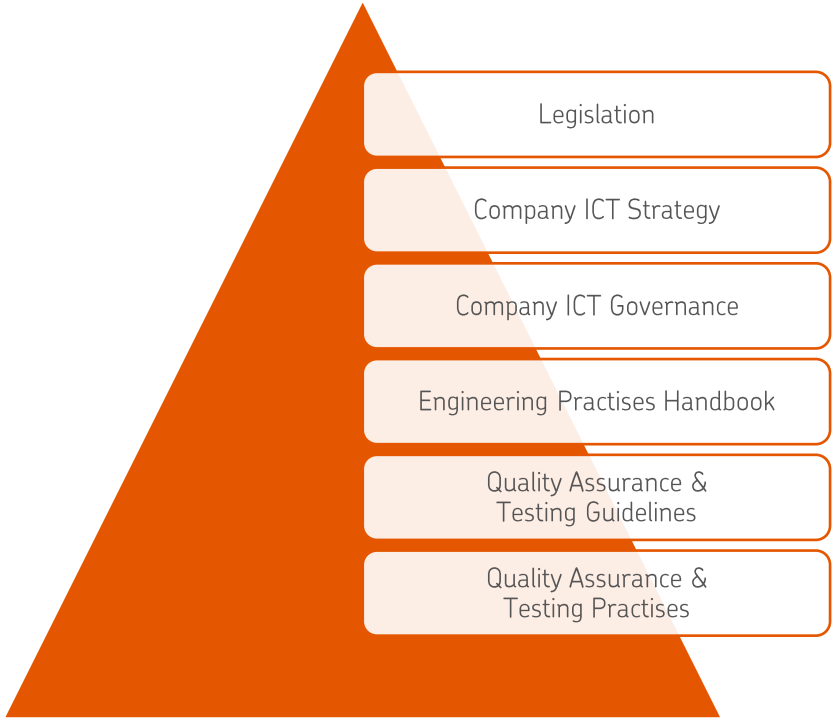
Aligning Learning Outcomes with Compliance Regulation

- ICT risk management and operational resilience testing are the key compliance areas that impact QA and security practices.
- Tailored course offerings that address regulatory needs while fostering strategic growth:
  - QA Security Testing – EU's Digital Operational Resilience Act (DORA*) requires a comprehensive digital operational testing programme as an integral part of a company's ICT risk-management framework. The testing programme should cover areas such as vulnerability assessments and scans, open-source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing. The learning supports DORA compliance.
  - CSA Sertificate of Cloud Security Knowledge CCSK - the CCSK certificate proves the skills in Zero Trust, DevSecOps, Cloud Telemetry and Security Analytics, Artificial Intelligence, and more. The learning supports OP Pohjola's cloud and AI journeys.

*REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector. Implementation date 17th January 2025. It covers: ICT risk management, ICT third-party risk management, Digital operational resilience testing, ICT-related incidents, Information sharing and Oversight of critical third-party providers.

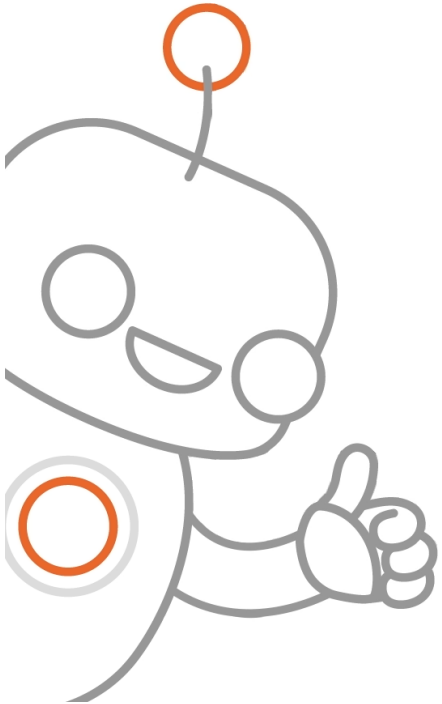
Strategic Goals and ICT Framework Integration

- **Alignment with ICT Strategy**
  - QA and Security learning paths align with ICT goals including cloud migration, AI-first development, and digital resilience.
- **Compliance Frameworks**
  - ICT Governance, Risk Management, and Digital Operational Resilience Testing program embed compliance into daily work practices to manage ICT risks.
- **Empowered Workforce**
  - Incorporating ICT frameworks into learning empowers employees to adapt to technological and regulatory changes.
- **Proactive Compliance Advantage**
  - Strategic integration turns compliance into a proactive strength, ensuring secure, high-quality services.



Summary

- Interdisciplinary learning bridges Quality Assurance and Cyber Security, supporting compliance and customer value.
- OP Tech Academy's tailored, adaptive learning paths empower employees to meet evolving regulatory and strategic demands.
- Collaboration between QA and Security ensures early risk detection, robust compliance, and continuous improvement.
- Embedding compliance and resilience into daily work transforms regulatory obligations into strategic strengths.
- Our approach prepares OP Financial Group to deliver secure, high-quality digital services in a rapidly changing environment.



Take-aways

- Break down silos: Foster collaboration between disciplines—security and quality are stronger together.
- Make learning continuous: Invest in your own growth and encourage adaptive, role-based learning in your teams.
- Turn compliance into opportunity: See regulatory demands as a driver for innovation, resilience, and customer trust.

Inspired? Connect and let's talk more

Mikko Paloheimo
Expert QA Lead, Chapter Lead and OP Tech Academy Headmaster at OP Financial Group

Michael Peltonen
Cyber Security Expert at OP Financial Group

Quality Assurance