

Organizational AI Security Champion Practice Course

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Organizational AI Security Champion Practice Course

Overview

Organizational AI Security Champion Practice Course is a one-week foundation course for security champions, cyber risk teams, IT managers, governance professionals, application owners, and business leaders, who leave with an AI Security Champion Action Plan. Participants discover AI assets and use cases, examine threat and misuse scenarios, coordinate data, prompt, access, and third-party controls, guide employees, and connect incidents, monitoring, awareness, and governance. Agile Leaders Training Center provides training in organizational AI security champion practice.

Who Should Attend

- Security champions responsible for connecting teams with security guidance and escalation
- Cyber risk teams responsible for identifying threats, controls, and monitoring needs
- IT management teams responsible for approved tools, access, and service oversight
- Governance teams responsible for policies, roles, evidence, and review gates
- Application owners responsible for AI use cases, data, suppliers, and user behavior
- Business leaders responsible for safe adoption and accountable decisions

The course assumes participants support AI adoption, security, risk, or governance decisions and leaves out coding, model development, penetration testing, detailed technical architecture, and vendor administration.

Departments and Industries

The course supports AI security champion practice across technology, risk, and business functions.

- Cybersecurity, information technology, and service management
- Risk, governance, privacy, legal, and internal control
- Operations, product, procurement, and transformation teams
- Financial services, healthcare, retail, and professional services
- Manufacturing, education, utilities, and public services

Learning Objectives

By the end of this course, participants will be able to:

- Build an inventory of AI assets and use cases
- Analyze threat, misuse, data, prompt, and supplier scenarios
- Apply access, review, monitoring, and escalation controls
- Evaluate secure-use guidance and employee awareness needs
- Build incident coordination and governance evidence
- Prioritize an AI security champion action plan

Course Agenda

Day 1: AI Asset and Use-Case Discovery

- AI Asset and Tool Inventory
- Business Use-Case and Owner Register
- Data Flow and Information Classification Map
- AI Dependency and Third-Party Profile
- Security Champion Stakeholder Network

Day 2: Threat and Misuse Scenario Analysis

- AI Threat and Misuse Scenario Canvas
- Prompt and Input Risk Checklist
- Data Exposure and Leakage Pathway Map
- Output Manipulation and Reliability Review
- Risk Likelihood and Impact Matrix

Day 3: Adoption Controls and Employee Guidance

- Approved AI Use and Data Boundary Guide
- Identity, Access, and Authorization Checklist
- Source Grounding and Content Filter Review
- Supplier Security Due-Diligence Questions
- Employee Secure-Use Conversation Guide

Day 4: Incidents, Monitoring, and Governance

- AI Security Signal and Monitoring Register
- Incident Triage and Escalation Pathway
- Human Approval and Override Decision Map
- AI Security Policy Evidence Checklist
- Control Owner and Review Calendar

AGILE LEADERS
Training Center

Day 5: Security Champion Practice

- Suggested Exercise: Discover AI Assets and Owners
- Suggested Exercise: Analyze Threat and Misuse Scenarios
- Suggested Exercise: Design Secure Adoption Guidance
- Suggested Exercise: Coordinate Incident and Governance Controls
- Capstone Exercise: AI Security Champion Action Plan

Practical Exercises

The course uses suggested activities to turn AI adoption concerns into visible security champion actions.

- Suggested activity: inventory tools, use cases, owners, data flows, dependencies, and stakeholders
- Suggested activity: assess threats, misuse, prompts, data exposure, outputs, and risk priority
- Suggested activity: design access, source, supplier, employee guidance, and monitoring controls
- Suggested activity: coordinate escalation, human approval, evidence, owners, reviews, and action priorities

FAQs

Who suits organizational AI security champion practice training?

Organizational AI security champion practice training suits security champions, cyber risk teams, IT managers, governance professionals, application owners, and business leaders. It assumes responsibility for safe AI adoption, not technical security testing or model development.

How does an AI security champion course differ from technical AI security engineering?

An AI security champion course focuses on discovery, business guidance, risk scenarios, control coordination, awareness, escalation, monitoring, and governance. Technical AI security engineering focuses more deeply on architecture, testing, implementation, and code-level defenses.

What should an organizational AI security champion inventory?

An organizational AI security champion should inventory tools, use cases, accountable owners, users, data flows, information classes, access paths, suppliers, dependencies, decisions, review points, monitoring signals, and escalation contacts.

How should AI security champions handle unapproved AI use?

AI security champions should document the use case, assess data and decision exposure, explain approved alternatives, involve accountable owners, route urgent risks through escalation, preserve evidence, and support proportionate remediation.

What evidence supports AI security governance?

AI security governance evidence includes inventories, ownership records, risk scenarios, access decisions, data boundaries, supplier reviews, user guidance, approvals, monitoring records, incidents, exceptions, corrective actions, and scheduled control reviews.

Conclusion

Participants take back an AI Security Champion Action Plan connecting assets, use cases, threats, data, prompts, access, suppliers, employee guidance, incidents, monitoring, and governance. It makes champion responsibilities and escalation paths visible. It supports safer adoption, consistent communication, control follow-through, and evidence-based review.

AGILE LEADERS
Training Center

Training Course Categories

- Agile PM and Project Management Training Courses
- Agribusiness & Food Security Training Courses
- Aviation Management and Operations Training Courses
- Certified Courses By International Bodies
- Communication and Public Relations Training Courses
- Crisis Management and Business Continuity Training Courses
- Data Analytics Training and Data Science Courses
- Digital Government & Public Service Training Courses
- Education and Learning Development Training Courses
- Environment & Sustainability Training Courses
- Facilities and Real Estate Training Courses
- Finance and Accounting Training Courses
- Governance, Risk and Compliance Training Courses
- Healthcare Management Training Courses
- Heritage Conservation and Museum Management Training Courses
- Hospitality and Tourism Training Courses
- Human Resources Training and Development Courses
- IT Security Training & IT Training Courses
- Leadership and Management Training Courses
- Legal Training, Procurement and Contracting Courses
- Maintenance Training and Engineering Training Courses
- Marketing, Customer Relations, and Sales Courses
- NGO, Humanitarian and Development Management Training Courses
- Occupational Health, Safety and Security Training Courses
- Oil & Gas Training and Other Technical Courses
- Personal & Self-Development Training Courses

AGILE LEADERS
Training Center

Training Course Categories

- Quality and Operations Management Training Courses
- Secretarial and Administration Training Courses
- Shipping, Maritime and Ports Training Courses

AGILE LEADERS
Training Center

Training Cities

Abu Dhabi UAE	**Accra** Ghana	**Addis Ababa** Ethiopia
Amman Jordan	**Amsterdam** Netherlands	**Athens** Greece
Baku Azerbaijan	**Bali** Indonesia	**Bangkok** Thailand
Barcelona Spain	**Berlin** Germany	**Cairo** Egypt
Cape town South Africa	**Casablanca** Morocco	**Chicago** USA
Doha Qatar	**Dubai** UAE	**Frankfurt** Germany
Geneva Switzerland	**Istanbul** Turkey	**Jakarta** Indonesia
Johannesburg South Africa	**Kuala Lumpur** Malaysia	**Kuwait** Kuwait
Lagos Nigeria	**Langkawi** Malaysia	**Lisbon** Portugal
London UK	**Madrid** Spain	**Manama** Bahrain
Marbella Spain	**Milan** Italy	**Montreux** Switzerland
Munich Germany	**Muscat** Oman	**Nairobi** Kenya

AGILE LEADERS
Training Center

Training Cities

New York USA	**Nice** France	**Paris** France
Phuket Thailand	**Port Louis** Mauritius	**Porto** Portugal
Prague Czech Republic	**Rome** Italy	**San Diego** USA
Seoul South Korea	**Sharm El-Sheikh** Egypt	**Singapore** Singapore
Tashkent Uzbekistan	**Tbilisi** Georgia	**Tokyo** Japan
Toronto Canada	**Trabzon** Turkey	**Vienna** Austria
Zanzibar Tanzania	**Zoom** Online Training	**Zurich** Switzerland