



Cyber Law and Digital Regulation Practice Training Course

22 – 26 August 2027
Nairobi

Cyber Law and Digital Regulation Practice Training Course

Ref: 762_157999 **Date:** 22 – 26 August 2027 **Location:** Nairobi **Fees:** 4500 Euro

Overview

Cyber Law and Digital Regulation Practice Training Course is a five-day intermediate course for legal, compliance, privacy, cybersecurity, governance, investigation, and policy functions who leave with a Cyber Legal Response Playbook. Participants map legal issues across digital evidence, incidents, privacy, contracts, platforms, third parties, and emerging technology without treating the course as legal advice. The course uses issue maps, decision records, clause reviews, and response scenarios. Agile Leaders Training Center develops cyber law and digital regulation practice.

Who Should Attend

- Legal functions responsible for advising on digital operations and disputes
- Compliance and privacy functions responsible for interpreting applicable duties
- Cybersecurity functions responsible for incidents, evidence, and control decisions
- Technology governance functions responsible for platforms, vendors, and emerging technology
- Investigation and policy functions responsible for records, escalation, and institutional response

The course assumes participants evaluate digital activities, controls, incidents, contracts, or evidence at work, and leaves out jurisdiction-specific legal advice, courtroom advocacy, technical forensics, and certification preparation.

Departments and Industries

The course supports departments and industries that manage legal exposure across digital operations.

- Legal, compliance, privacy, and internal assurance
- Cybersecurity, technology governance, and digital operations
- Financial services and insurance
- Healthcare, education, and public services
- Technology platforms, telecommunications, and professional services

Learning Objectives

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



- Apply a cyber legal issue-spotting method
- Analyze digital evidence and preservation decisions
- Evaluate privacy, incident, and disclosure duties
- Use contract and third-party risk clause checklists
- Compare platform and emerging-technology legal risks
- Build a Cyber Legal Response Playbook

Course Agenda

Day 1: Map Cyber Legal Issues

- Cyber Law Scope and Issue Map
- Jurisdiction and Cross-Border Factor Matrix
- Legal Duty, Risk, and Stakeholder Register
- Digital Rights and Responsibility Decision Card
- Legal Assumption and Advice Boundary Log

Day 2: Handle Digital Evidence

- Cybercrime and Electronic Evidence Issue Tree
- Evidence Relevance and Admissibility Question Set
- Preservation and Chain-of-Custody Checklist
- Cross-Border Evidence Cooperation Map
- Investigation Record and Escalation Template

Day 3: Evaluate Data and Incident Duties

- Privacy and Data-Handling Obligation Matrix
- Incident Notification Trigger Checklist
- Disclosure, Confidentiality, and Privilege Decision Map
- Data Retention and Deletion Control Review
- Incident Legal Decision Record

Day 4: Govern Contracts and Technology

- Digital Contract Formation and Signature Checklist
- Technology Neutrality and Functional Equivalence Test
- Third-Party Cyber Clause Review Matrix
- Platform Content and Intermediary Risk Map
- Automated Contracting and Emerging Technology Register



Day 5: Practice Cyber Legal Response

- Exercise: Diagnose a Cross-Border Cyber Legal Scenario
- Exercise: Evaluate Digital Evidence and Preservation Choices
- Exercise: Test Incident, Privacy, and Disclosure Decisions
- Exercise: Review Contract and Platform Risk Controls
- Capstone: Cyber Legal Response Playbook

Practical Exercises

The course uses suggested activities based on financial services, healthcare, technology platforms, and professional services.

- Suggested activity: map parties, jurisdictions, duties, evidence, and unanswered legal questions in an incident scenario.
- Suggested activity: document preservation, custody, confidentiality, escalation, and disclosure choices for digital evidence.
- Suggested activity: review a third-party cyber clause pack and record negotiation priorities.
- Suggested activity: present a legal response playbook with assumptions, triggers, owners, and decision records.

FAQs

Who suits cyber law and digital regulation training, and what does it assume?

Legal, compliance, privacy, cybersecurity, governance, investigation, and policy functions suit the course; it assumes responsibility for evaluating digital activities, duties, incidents, contracts, controls, or evidence.

How does cyber law training differ from technical cybersecurity training?

Cyber law training evaluates legal duties, rights, evidence, contracts, and response decisions, while technical cybersecurity training focuses on designing, operating, testing, or defending systems.

How should cyber law teams assess digital evidence?

Cyber law teams should record relevance, source, integrity, preservation, custody, access, confidentiality, jurisdiction, authority, transfer, limitations, and the questions requiring qualified legal advice.

What should cyber law incident decision records contain?

Cyber law incident records should state known facts, assumptions, applicable duty categories, trigger analysis, options, approvals, evidence impact, confidentiality, communications, deadlines to verify, owners, and follow-up actions.



How do digital regulations affect technology contracts?

Digital regulations affect allocation of security duties, data handling, incident cooperation, audit evidence, subcontracting, access, retention, deletion, intellectual property, service changes, liability, and termination assistance.

Conclusion

Participants take back a Cyber Legal Response Playbook connecting issue spotting, evidence, incidents, privacy, contracts, platforms, third parties, and emerging technology. It changes fragmented legal questions into traceable decision routes. The playbook supports early escalation, documented assumptions, cross-functional coordination, clause review, and referral for jurisdiction-specific advice.