JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

# Digital Risk Controls for Information Systems Training Course

16 – 20 August 2027
Rome

# Digital Risk Controls for Information Systems Training Course

**Ref:** 3117_118316 **Date:** 16 – 20 August 2027 **Location:** Rome **Fees:** 7200 GBP

Digital Risk Controls for Information Systems is a 1-week training course for risk, internal control and information security officers that ends with a digital risk control matrix for one information system. As systems spread across cloud hosting, suppliers and remote access, organisations must show that each control works, not merely that it exists. Jupiter Prime Training treats digital risk controls as shared work of risk, control and security functions.

## Why Digital Risk Controls Matter Now

Three forces shape digital risk controls today. Core processes now run on hosted platforms and supplier services, so the control boundary no longer matches the organisation's own network. Audit committees and external assurers expect evidence that controls operate over time, not policy statements. Attackers also target credentials, moving attention to access rights. An organisation that links each information asset to tested controls responds to incidents with clarity; one that relies on untested settings discovers its gaps during an audit or a breach.

## Who Gains Most from Digital Risk Controls

- Officers who maintain the risk register for information assets and rate inherent and residual exposure
- Internal control specialists who design, document and test automated and manual system controls
- Information security officers responsible for access rules, encryption settings and alert handling
- Assurance reviewers who sample control evidence and report deficiencies to audit committees
- Supplier oversight leads who assess hosted services and outsourced system operations

The strongest results come when a risk function, its internal control colleagues and the security team attend together.

## Digital Risk Controls Capabilities

Participants move from listing threats to proving that specific safeguards reduce exposure on a named system.

- Assess information assets by confidentiality, integrity and availability impact — the risk owner's treatment decision
- Design preventive, detective and corrective controls for access and encryption — the system owner
- Specify logging and monitoring rules that produce usable alerts — the security operations lead
- Test supplier and hosted service controls against contract terms — the procurement and supplier oversight function
- Build control evidence files that withstand sampling — internal and external assurance reviewers
- Communicate control deficiencies with rated severity and remediation owners — the audit committee

## Key Digital Risk Controls Terms

- Information Asset — any data set, application or service whose loss, alteration or unavailability would harm the organisation's operations or obligations.
- Residual Risk — the exposure that remains after existing controls are applied, compared against the organisation's stated risk appetite.
- Least Privilege — the principle that each user or service account holds only the access rights its current task requires.
- Control Operating Effectiveness — evidence that a control performed as designed throughout a period, not only at a single point in time.
- Shared Responsibility Model — the division of security duties between a hosted service provider and the customer organisation using it.
- Compensating Control — an alternative safeguard that reduces a risk when the preferred control cannot be applied in full.

## Digital Risk Controls Day by Day

## Day 1: Mapping Information Assets and Exposure

- Information Asset Inventory — Which Systems Hold Critical Records
- Impact Rating by Confidentiality, Integrity and Availability — Treatment Priority
- Threat and Vulnerability Pairing — Realistic Loss Scenarios for Each Asset
- Inherent Versus Residual Risk Scoring — Appetite and Tolerance Limits
- Risk Owner Assignment — Accountability for Each System's Exposure

## Day 2: Access and Encryption Safeguards

- Role-Based Access Design and Least Privilege — Joiner, Mover, Leaver Rules
- Privileged Account Oversight — Approval and Session Recording Choices
- Periodic User Access Recertification — Removing Excess Rights on Time
- Encryption at Rest and in Transit — Key Custody and Rotation
- Segregation of Duties Conflict Matrix — Fraud and Error Prevention

## Day 3: Logging, Monitoring and Detection

- Log Source Selection and Retention Rules — Investigation Readiness
- Alert Thresholds and Use Cases — Reducing Noise for Analysts
- Change and Configuration Monitoring — Detecting Unapproved System Changes
- Incident Escalation Paths — Who Decides Containment and Disclosure
- Control Performance Indicators — Reporting Detection Health to Leadership

## Day 4: Supplier, Hosted Service and Evidence Testing

- Shared Responsibility Mapping — Which Duties Stay With the Organisation
- Supplier Assurance Report Review — Relying on Third-Party Attestations
- Contract Security Clauses and Right to Audit — Supplier Oversight Leverage
- Test of Design Versus Test of Operation — Sampling Method Choice
- Control Evidence File Structure — Withstanding Assurance Review Sampling

## Day 5: Practising the Digital Risk Control Matrix

- Asset and Exposure Profile for a Chosen System — Scope Agreement
- Access, Encryption and Monitoring Controls Mapped to Risks — Coverage Gaps
- Compensating Controls and Deficiency Ratings — Remediation Sequencing
- Peer Challenge of Control Evidence — Readiness for Assurance Sampling
- Completed Digital Risk Control Matrix — Sign-Off by the System Owner

## Applying Digital Risk Controls After the Course

- Run a user access recertification on one critical application and record removed rights as control evidence.
- Compare one hosted service's assurance report with the shared responsibility map and log any uncovered duties.

## Digital Risk Controls Questions FAQ

### What are digital risk controls for information systems and why do they matter now?

Digital risk controls are the safeguards that reduce exposure on data, applications and services. They matter now because systems run across suppliers and hosted platforms, and boards expect evidence that each safeguard operates, not just a written policy.

### Which roles gain most from digital risk controls training?

Risk officers, internal control specialists and information security officers gain most. Supplier oversight leads and assurance reviewers also benefit from the shared control set.

## How does a digital risk controls course differ from a general cyber security course?

It focuses on control design, testing and evidence rather than technical defence tooling. You work on rating exposure, mapping safeguards to risks and proving operation to assurers.

## What do you bring back from digital risk controls training?

You bring back a completed control matrix for one information system, with rated risks, mapped safeguards, evidence references and remediation owners.

## Digital Risk Controls: The Way Forward

The digital risk control matrix first informs which deficiencies the system owner funds and fixes first. Risk officers use it to update residual ratings, security teams use it to tune monitoring, and assurance reviewers use it to plan sampling. After its first use, revisit how hosted service duties are split, since supplier changes shift the control boundary quickly.