JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Records Security Controls and Information Classification Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Records Security Controls and Information Classification Training Course

Records Security Controls and Information Classification is a 1-week training course for records managers, IT staff and compliance officers, in which each participant builds a records security control matrix for their organisation. Sensitive files now sit across email, shared drives and cloud platforms, so a single misplaced permission can expose personnel, client or contract evidence. Jupiter Prime Training runs this course for teams that guard such holdings.

Why Records Security Controls and Information Classification Matter Now

Three pressures shape this subject today. Attackers target file shares and mailboxes because records hold what is worth stealing or ransoming. Data-protection and litigation duties expect organisations to show who could open a sensitive file and when. Hybrid working spreads copies across personal devices and guest links. Organisations that label holdings by sensitivity and match controls to each label contain incidents quickly and defend their decisions; those that do not over-lock routine files and under-protect critical ones. The course draws on ISO 15489-1 for records principles and ISO 16175 for the security functions a records platform should provide.

Who Gains Most from Records Security Controls and Information Classification

- Records leads who own file plans, retention rules and access to archives
- Systems staff who configure permissions, encryption and audit logging on storage platforms
- Compliance specialists who map legal duties and evidence demands to record holdings
- Risk coordinators who rate the impact of lost or leaked records
- Department custodians who approve who may see restricted case files

A joint group of records, IT and compliance staff from one organisation gains most because the three functions must agree on labels and owners.

Records Security Controls and Information Classification Capabilities

Participants learn to connect sensitivity labels with the permissions, logs and response steps that protect each class of record.

- Design a sensitivity labelling scheme for records — information owners
- Assess access rights against need-to-know rules — department heads
- Specify encryption, logging and retention settings per label — systems staff
- Weigh legal hold and disclosure risk for sensitive files — legal counsel
- Build a records breach response sequence — incident leads
- Communicate control gaps and remediation priorities — senior risk committees

Key Records Security Controls and Information Classification Terms

- Sensitivity label — a marking such as public, internal, confidential or restricted that tells handlers how a record must be protected.
- Need-to-know — the rule that access is granted only to people whose duties require that specific record.
- Access control list — the set of users and groups allowed to open, edit or delete a file or folder.
- Audit trail — a tamper-evident log showing who viewed, changed, moved or deleted a record and when.
- Legal hold — an instruction suspending disposal of records relevant to litigation, investigation or audit.
- Records breach — any loss, unauthorised disclosure or corruption of records, whether caused by attack, error or theft.

Records Security Controls and Information Classification Day by Day

Day 1: Threats to Record Holdings

- Threat Landscape for File Shares and Mailboxes — Which Holdings Attract Attackers
- Records Principles From ISO 15489-1 — Authenticity, Integrity and Reliability Needs
- Records Holdings Inventory — Where Sensitive Files Actually Reside
- Insider Misuse and Accidental Exposure Patterns — Priority Risk Scenarios
- Legal and Contractual Protection Duties — Evidence Regulators and Courts Expect

Day 2: Classifying by Sensitivity

- Four-Tier Sensitivity Scheme — Labels Staff Can Apply Consistently
- Impact Rating of Loss or Leak — Assigning Each Record Series a Tier
- Information Owner Assignment — Who Approves Label and Access Decisions
- Marking Methods in Email, Documents and Metadata — Visible Handling Signals
- Reclassification and Downgrading Triggers — When Sensitivity Expires

Day 3: Access and Technical Safeguards

- Role-Based Permission Design — Least Privilege for Each Record Series
- Encryption at Rest and in Transit — Protecting Restricted Tiers
- Audit Logging Settings From ISO 16175 — Evidence of Every Access Event
- Guest Links, Removable Media and Personal Devices — Sharing Boundaries
- Periodic Access Recertification — Removing Leavers and Role Movers

Day 4: Legal Risk and Breach Response

- Legal Hold Procedure — Freezing Disposal During Disputes
- Disclosure and Subject Access Requests — Releasing Only What Is Required
- Breach Triage Checklist — Containing a Records Exposure in Hours
- Notification Decision Tree — When Owners, Clients and Authorities Are Told
- Post-Incident Lessons Log — Fixing the Control That Failed

Day 5: Practising the Records Security Control Matrix

- Applying Sensitivity Tiers to a Finance and Healthcare Case — Label Choices
- Testing Permission Designs Against a Mock Audit Trail — Gap Findings
- Rehearsing a Breach Scenario With Legal Hold — Response Timing
- Prioritising Remediation by Impact and Effort — Funding Sequence
- Completing the Records Security Control Matrix — Owner Sign-Off

Applying Records Security Controls and Information Classification After the Course

- Run a sensitivity labelling pass on one high-risk record series and confirm owners for each tier.
- Recertify access on one shared drive or team site against need-to-know rules and record the permissions removed.

Records Security Controls and Information Classification Questions FAQ

What are Records Security Controls and Information Classification and why do they matter now?

They are the labels, permissions, logs and response steps that protect records according to sensitivity. They matter now because files spread across cloud platforms and devices, and organisations must show who could reach sensitive evidence.

Which roles gain most from Records Security Controls and Information Classification?

Records managers, systems staff and compliance specialists gain most. Each owns one part of the controls.

How does Records Security Controls and Information Classification differ from a general cyber security course?

It focuses on protecting records rather than networks. It covers labels, need-to-know access, legal hold and breach response rather than firewalls and endpoints.

What do you bring back from Records Security Controls and Information Classification?

You bring back a control matrix linking each record series to a sensitivity tier, owner, permissions, logging and response steps, ready for sign-off by your risk or compliance committee.

Records Security Controls and Information Classification: The Way Forward

The records security control matrix links each record series to a sensitivity tier, an owner, permissions, logging and breach steps. Its first use is to decide which restricted holdings need encryption and access recertification first. Records leads, systems staff and compliance specialists maintain it together. Revisit tiers after the first breach drill, since real response timing shows whether labels and controls match the risk.