JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

EDMS Backup and Restoration Strategies Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

EDMS Backup and Restoration Strategies Training Course

EDMS Backup and Restoration Strategies is a 1-week training course for EDMS administrators, IT support staff and records managers, in which each participant writes an EDMS backup and restore runbook. Ransomware, failed upgrades and accidental deletions threaten stores of contracts, drawings and patient files, and a restore that loses metadata can leave records unusable as evidence. Jupiter Prime Training delivers this course for practitioners responsible for repository recovery.

Why EDMS Backup and Restoration Strategies Matter Now

Three forces raise the stakes for EDMS recovery. Ransomware attacks target file shares and databases together, so a backup kept on the same network may be encrypted alongside the live repository. Upgrades and cloud migrations add moments of corruption risk. Records managers also need restored documents to keep their metadata, versions and audit trails, or the files lose value as evidence. Organisations that test restores regularly resume work in hours; those that never test discover gaps during an outage. The course draws on ISO 15489-1 for authenticity and integrity of records and ISO 16175 for the functional requirements of records software.

Who Gains Most from EDMS Backup and Restoration Strategies

- Administrators who schedule, monitor and verify repository backups
- Support staff who perform restores of files, folders and databases
- Records specialists who confirm that restored items keep metadata and history
- Infrastructure practitioners who manage storage, replication and offsite copies
- Coordinators who log incidents and communicate recovery progress to users

An IT and records pairing responsible for one document platform gains most when an administrator and a records specialist attend together.

EDMS Backup and Restoration Strategies Capabilities

Each capability links a backup decision to what a user or auditor finds after a restore.

- Specify recovery point and recovery time objectives for each document library — business owners and the records manager
- Design a backup schedule mixing full, incremental and differential copies — the infrastructure and storage owner
- Apply restore procedures for single files, folders, metadata databases and whole repositories — support staff and administrators
- Test restores against a checklist that confirms versions, permissions and audit trails — records managers and internal auditors
- Assess immutable, offline and offsite copies against ransomware scenarios — information security leads
- Communicate recovery steps and progress through a written runbook — users, managers and incident coordinators

Key EDMS Backup and Restoration Strategies Terms

- Recovery point objective — the maximum period of document changes that may be lost after an incident.
- Recovery time objective — the target time within which a repository must be available again after a failure.
- Incremental backup — a copy of only the items changed since the previous backup of any type.
- Immutable backup — a copy that cannot be altered or deleted for a set period, protecting it from ransomware.
- Content store — the file storage that holds document binaries, separate from the database holding their metadata.
- Restore test — a planned recovery of sample content confirming backups are usable.

EDMS Backup and Restoration Strategies Day by Day

Day 1: Risks and Recovery Targets

- EDMS Architecture for Recovery — Database, Content Store, Index and Configuration
- Threat Scenarios — Ransomware, Corruption, Deletion and Failed Upgrades
- Recovery Point and Recovery Time Objectives — Setting Targets per Library
- Business Impact Assessment — Ranking Repositories by Criticality
- Records Integrity Principles From ISO 15489-1 — Authenticity After Recovery

Day 2: Backup Types and Schedules

- Full, Incremental and Differential Backups — Balancing Storage and Speed
- Snapshot and Replication Options — When Copies Are Not Backups
- The Three-Two-One Rule — Copies, Media and Offsite Locations
- Immutable and Offline Copies — Defending Backups Against Ransomware
- Backup Monitoring and Alerts — Catching Silent Failures Early

Day 3: Restoring Repositories and Metadata

- Single Item and Folder Restore — Recovering From User Deletion
- Metadata Database Restore — Keeping Documents and Profiles in Step
- Search Index Rebuild — Restoring Findability After Recovery
- Version History and Audit Trail Recovery — Preserving Evidence Value
- Permission and Configuration Restore — Returning Access Rules Correctly

Day 4: Testing and Recovery Decisions

- Restore Test Design — Samples, Frequency and Pass Criteria
- Integrity Checks — Hashes, Counts and Spot Checks After Restore
- Functional Requirements From ISO 16175 — What Records Software Must Keep
- Incident Escalation — Deciding Between Partial and Full Recovery
- Recovery Communication — Messages to Users, Managers and Auditors

Day 5: Practising the EDMS Backup and Restore Runbook

- Ransomware Scenario — Applying Day Two Defences to a Hospital Repository
- Restore Drill — Applying Day Three Steps to an Engineering Drawing Library
- Test Review — Applying Day Four Checks to a Public Records Archive
- Lessons Log — Recording Gaps Found During Drills
- EDMS Backup and Restore Runbook — Targets, Schedules, Restore Steps and Tests

Applying EDMS Backup and Restoration Strategies After the Course

- Agree recovery targets with the owners of two critical document libraries and record them in the runbook.
- Run a restore test of sample folders against the integrity checklist and log the gaps found.

EDMS Backup and Restoration Strategies Questions FAQ

What are EDMS backup and restoration strategies and why do they matter now?

EDMS backup and restoration strategies are the planned ways of copying a document repository and recovering it with metadata and history intact. They matter now because ransomware, upgrades and migrations make repository failures more likely and more damaging.

Which roles gain most from EDMS backup and restoration strategies training?

EDMS administrators, IT support staff and records managers gain most. Security practitioners sharing platform duties also benefit.

How does an EDMS backup and restoration strategies course differ from a general IT disaster recovery course?

An EDMS backup and restoration strategies course focuses on document repositories, where metadata, versions and audit trails must survive recovery. A general disaster recovery course covers whole data centres without that records focus.

What do you bring back from EDMS backup and restoration strategies training?

You bring back a written runbook with recovery targets, backup schedules, restore steps and test checklists, ready for your IT and records colleagues.

EDMS Backup and Restoration Strategies: The Way Forward

The EDMS backup and restore runbook sets recovery targets, backup schedules, restore steps and test routines for one repository. Its first use is agreeing recovery point and recovery time objectives with library owners, led by the EDMS administrator with the records manager. Revisit it after the first full restore test, when real timings show whether the targets are achievable.