JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

# Data Warehouse Security and Data Management Essentials Training Course

23 – 27 August 2027
Rome

# Data Warehouse Security and Data Management Essentials Training Course

**Ref:** 2977_112841 **Date:** 23 – 27 August 2027 **Location:** Rome **Fees:** 7200 GBP

Data Warehouse Security and Data Management Essentials is a 1-week training course for data managers, administrators and information security staff, ending with a secure data warehouse plan. Central analytical stores now gather finance, customer and employee records in one place, which makes them valuable to decision makers and attractive to attackers alike. Jupiter Prime Training offers this course on Data Warehouse Security and Data Management Essentials.

## Why Data Warehouse Security and Data Management Essentials Matters Now

Three pressures shape this work. More departments demand self-service access to the central store, multiplying permissions to approve. Feeds from cloud applications and partners bring records in through connections that are easily forgotten. Auditors and boards ask who can see sensitive fields and how quickly the store could be restored after corruption or ransomware. An organisation that classifies, restricts and backs up its warehouse sensibly keeps reporting trusted; one that does not risks leaked salaries, altered figures and lost history that cannot be rebuilt.

## Who Gains Most from Data Warehouse Security and Data Management Essentials

- Those who approve and review access requests to reporting stores
- Those who run loads, schedules and storage for the central warehouse
- Those who assess security risks and monitor suspicious activity on data platforms
- Those who own source systems feeding records into the warehouse

A business intelligence unit gains most when its administrator, a security analyst and a data owner attend together, because permission design and integration controls are then agreed by the people who enforce them.

## Data Warehouse Security and Data Management Essentials Capabilities

Participants link each sensitivity label to a concrete control, from column masking to restore testing.

- Assess warehouse holdings against a sensitivity scheme — data owners setting handling rules
- Design role-based permissions with row and column restrictions — administrators granting access
- Specify encryption and masking for sensitive fields — security staff and auditors
- Build a backup and restore routine with tested recovery targets — continuity planners
- Apply secure integration checks to incoming feeds — source system owners
- Communicate warehouse risk and control status — senior management and audit committees

## Key Data Warehouse Security and Data Management Essentials Terms

- Data classification — labelling records by sensitivity, such as internal or restricted, each with handling rules.
- Role-based access — granting permissions to job roles rather than individuals.
- Row-level restriction — a rule that limits which records a user sees, for example only their own region.
- Data masking — replacing sensitive values with realistic substitutes.
- Recovery point objective — the maximum period of recent changes an organisation accepts losing after a failure.
- Staging area — a holding zone where incoming records are checked and cleaned before entering the main store.

## Data Warehouse Security and Data Management Essentials Day by Day

### Day 1: Warehouse Purpose and Threat Landscape

- Warehouse Layer Map From Staging to Reporting — Locating Where Sensitive Records Sit
- Threat Scenarios for Analytical Stores — Prioritising Insider Misuse, Leakage and Corruption
- Data Owner and Custodian Duties — Assigning Accountability for Each Subject Area
- Sector Cases in Healthcare and Banking — Comparing Consequences of Exposed Reporting Data
- Control Baseline Checklist — Recording Current Protections Before Change

### Day 2: Classification and Access Design

- Sensitivity Labelling Scheme — Setting Handling Rules for Every Table and Column
- Role Catalogue and Permission Matrix — Granting Access by Job Rather Than Person
- Row and Column Restrictions — Limiting Views to What Each Role Needs
- Access Request and Recertification Routine — Removing Stale or Excess Permissions
- Privileged Account Controls — Watching Administrators and Service Accounts Closely

### Day 3: Protecting Stored Records

- Encryption at Rest and in Transit — Choosing Protection for Files and Connections
- Masking and Tokenisation Options — Letting Analysts Work Without Seeing Originals
- Activity Logging and Alert Rules — Detecting Unusual Queries and Bulk Exports
- Backup Schedule and Retention Tiers — Matching Copies to Recovery Point Targets
- Restore Rehearsal Script — Proving the Store Can Return After Corruption

### Day 4: Secure Integration and Change

- Source Feed Inventory and Trust Levels — Deciding Which Connections Need Extra Checks
- Staging Validation Rules — Rejecting Malformed or Tampered Incoming Records
- Credential Storage for Load Jobs — Removing Passwords From Scripts and Schedules
- Change Approval for Schema and Permissions — Preventing Silent Exposure Through Updates
- Third-Party Connection Agreements — Setting Security Terms With Feed Providers

## Day 5: Practising the Secure Data Warehouse Plan

- Classification of a Sample Subject Area — Applying Day Two Labels to Real Tables
- Permission Matrix Walk-Through — Testing Roles Against Typical Requests
- Backup and Restore Gap Review — Comparing Current Copies With Recovery Targets
- Control Status Scorecard — Reporting Warehouse Risk to Senior Management
- Secure Data Warehouse Plan — Sequencing Controls, Owners and Review Dates

## Applying Data Warehouse Security and Data Management Essentials After the Course

- Label one subject area and remove permissions the matrix shows are unnecessary.
- Run the restore rehearsal on a test copy and record recovery time against target.

## Data Warehouse Security and Data Management Essentials Questions FAQ

### What is Data Warehouse Security and Data Management Essentials and why does it matter now?

It is the set of controls that classify, restrict, back up and safely feed a central analytical store. It matters now because more people and systems reach the warehouse, raising the chance of leaks and corrupted reporting.

### Which roles gain most from Data Warehouse Security and Data Management Essentials?

Warehouse administrators, information security analysts and data owners gain most. Anyone approving access or answering audit questions applies the methods directly.

### How does Data Warehouse Security and Data Management Essentials differ from an advanced warehouse engineering course?

This course works at foundation level on protection: classification, permissions, backup and safe integration. An advanced engineering course concentrates on storage architecture and modelling choices for performance and scale.

### What do you bring back from Data Warehouse Security and Data Management Essentials?

You bring back a sensitivity scheme, a permission matrix, a restore rehearsal script and a sequenced control plan, each drafted around your own warehouse.

## Data Warehouse Security and Data Management Essentials: The Way Forward

The secure data warehouse plan gives administrators and security staff an ordered list of controls with named owners. Its first use is deciding which subject areas receive masking and tighter permissions. Data owners and senior management track it through the control scorecard, and it deserves revisiting after the first restore rehearsal or audit finding.