Confidentiality Policy Design, Breach Response and Assurance Training Course for Senior Managers

11 – 15 January 2027
Rome

Confidentiality Policy Design, Breach Response and Assurance Training Course for Senior Managers

Ref: 309_20981 **Date:** 11 – 15 January 2027 **Location:** Rome **Fees:** 5500 GBP

Programme Summary

Confidentiality policy design is the subject of this one-week training course for senior managers in compliance, legal, human resources and operations, ending in a confidentiality policy and breach response pack for one organisation. Confidential information leaves organisations through ordinary routes such as email, suppliers and departing staff, and weak rules make a breach harder to contain. The programme moves from classifying information and setting access rules, through breach response, to assurance of compliance standards, and then to a worked pack. Mars Training Centre UK delivers this programme in confidentiality policy and breach response.

The Business Case

Most confidentiality failures are not attacks but lapses: a file sent to the wrong recipient, a supplier given wider access than needed, a leaver who keeps documents. A confidentiality policy that classifies information, limits access to need and sets out a tested response lets managers contain a breach quickly and show boards and counterparties that the rules are applied rather than only written.

- Breach Containment Time: Shortens as roles, notification steps and evidence handling are agreed in advance.
- Access Exposure: Falls as information is classified and access follows need to know.
- Assurance Confidence: Improves as compliance with the policy is sampled and reported to a committee.

Principles and Evidence Base

- ISO/IEC 27001: Its approach to information security management and access control guides the classification and access work in Sessions 1 and 2.
- ISO 37301: Its compliance management system concepts structure the monitoring and assurance work in Session 4.
- Information Classification: Grading information as public, internal, confidential or restricted guides the policy design in Session 1.

Intended Participants

- Compliance and ethics leaders who own the confidentiality policy.
- Legal and contracts managers who draft confidentiality terms with staff and suppliers.
- Human resources leaders who manage joiners, movers and leavers.
- Operations and security managers who apply access rules and respond to incidents.

The programme serves banking, healthcare, professional services and public-sector organisations that hold sensitive information.

Learning Outcomes

1. Participants will be able to classify organisational information and assign handling rules to each class.
2. Participants will be able to construct a confidentiality policy with access, disclosure and exception rules.
3. Participants will be able to diagnose confidentiality gaps in supplier, staff and meeting practices.
4. Participants will be able to prioritise the steps of a breach response and assign owners to them.
5. Participants will be able to evaluate compliance with the policy using samples and indicators.
6. Participants will be able to justify a confidentiality policy and breach response pack to a senior committee.

Programme Structure

Day 1: Confidentiality Policy Foundations

What information needs protecting, and under which rules?

- Information Asset Inventory
- Information Classification Scheme
- Handling Rules by Class
- Policy Scope and Ownership Statement
- Confidentiality Policy Structure

Day 2: Access, Disclosure and Third Parties

Who may see confidential information, and on what terms?

- Need-to-Know Access Matrix
- Confidentiality Terms for Staff and Suppliers
- Joiner, Mover and Leaver Checklist
- Disclosure and Exception Approval Process
- Meeting and Document Sharing Rules

Day 3: Breach Response

What happens in the first day after a confidentiality breach?

- Breach Definition and Severity Scale
- Detection and Reporting Channels
- Containment and Evidence Handling Steps
- Notification Decision Tree
- Post-Breach Review Template

Day 4: Compliance Standards and Assurance

How does management know the policy is followed?

- Compliance Obligations Register
- Sample-Based Compliance Testing
- Compliance Indicator Set
- Corrective Action Tracking
- Committee Reporting Format

Day 5: Applying the Confidentiality Policy to One Organisation

Is the confidentiality policy and breach response pack ready for the senior committee?

- Classifying Sample Records Using Session 1 Rules
- Testing Access Rules Against Session 2 Cases
- Walking a Simulated Breach Through Session 3 Steps
- Selecting Session 4 Indicators for the Pack
- Completing the Confidentiality Policy and Breach Response Pack

Methodology

The programme is built around structured exercises and case analysis. Participants work with anonymised policy extracts, incident summaries and supplier terms, classify information, test access rules and run a simulated breach in small teams, then present their pack to a mock committee. No technical background in information security is required.

- Suggested activity: Classifying a mixed set of fifteen sample records.
- Suggested activity: Reviewing a supplier confidentiality clause for gaps.
- Suggested activity: Running a timed breach response simulation with assigned roles.

Capstone Output

Each participant completes a confidentiality policy and breach response pack for one organisation. It contains a classification scheme, an access matrix, confidentiality terms, a breach response plan, a set of compliance indicators and a short note for the senior committee. It is used to brief the committee, to update contracts and to plan the first assurance review.

Frequently Asked Questions

Is confidentiality policy training suitable for managers without a security background?

Yes. Confidentiality policy training is set at managerial level and assumes responsibility for compliance, legal, people or operations, not technical security expertise.

Which standards does the confidentiality policy work rest on in this programme?

The confidentiality policy work rests on ISO/IEC 27001 for information security management, ISO 37301 for compliance management systems and a four-level information classification.

How is the confidentiality policy and breach response pack used at work?

You use the confidentiality policy and breach response pack to brief the committee, update staff and supplier terms and plan the first assurance review.

How does a confidentiality policy differ from a data protection programme?

A confidentiality policy governs access to and disclosure of all sensitive information, while a data protection programme concentrates on personal data and the rights of individuals.