CONCEPT

Cyber Risk Management and Digital Asset Protection Training: Essential Controls and Incidents



Cyber Risk Management and Digital Asset Protection Training: Essential Controls and Incidents

Introduction:

Cyber Risk Management and Digital Asset Protection Training: Essential Controls and Incidents is a 3-day course for department managers, IT and security officers, risk and compliance staff and information asset owners, ending with a Digital Asset Risk and Incident Readiness Register for one unit. Many units cannot say which systems and data they hold or which safeguards protect them, so weaknesses surface only during an incident. Nominees already manage or support systems and information in their unit and practise on case studies from several sectors. CoreConcept Training Center delivers this cyber risk management and digital asset protection course.

Course Objectives:

- Build a digital asset inventory that records owners, locations and classification levels for systems and data
- Assess cyber risks to each asset by linking threats and vulnerabilities to likelihood and impact scores
- Select essential safeguards from CIS Controls v8.1 Implementation Group 1 for the highest-scoring risks
- Map unit controls to the NIST CSF 2.0 functions and the ISO/IEC 27001:2022 control themes
- Apply the incident handling steps of detection, reporting, containment, recovery and lessons learned
- Produce a Digital Asset Risk and Incident Readiness Register with owners and follow-up actions

Target Audience:

- Department managers responsible for the systems, data and staff access within their unit
- IT and security officers responsible for configuring, patching and monitoring business systems
- Risk and compliance staff responsible for recording risks and checking that controls operate
- Information and data owners responsible for deciding classification and access to records
- Business continuity and operations coordinators responsible for restoring services after disruption

Course Outline:

Day 1: Digital Asset Inventory and Cyber Risk Foundations

- NIST CSF 2.0 Six Functions for Unit-Level Protection
- Digital Asset Inventory Template for Hardware, Software and Data
- Information Classification Scheme and Asset Owner Assignment
- Threat and Vulnerability Catalogue for Common Business Systems
- Cyber Risk Register Scoring by Likelihood and Impact

Day 2: Essential Security Controls and Incident Handling Steps

- CIS Controls v8.1 Implementation Group 1 Safeguard Selection
- Access Control Review and Multi-Factor Authentication Coverage Checks
- Patch, Backup and Secure Configuration Verification Checklists
- ISO/IEC 27001:2022 Control Themes Mapped to Unit Risks
- NIST SP 800-61 Rev. 3 Incident Handling and Reporting Flow

Day 3: Case Study Practice and the Readiness Register

- Case Study Phishing-Led Account Compromise in a Finance Unit
- Case Study Ransomware Outage in a Service Operations Centre
- Containment, Recovery and Lessons Learned Log Completion
- Staff Awareness Plan Linked to Recorded Incident Causes
- Digital Asset Risk and Incident Readiness Register Completion

Skills You Will Gain:

- Digital Asset Inventory Management
- Information Classification
- Cyber Risk Scoring
- Security Control Selection
- Access Review Practice
- Backup and Patch Verification
- Incident Triage and Reporting
- Lessons Learned Analysis

Why Attend This Course:

- Deliver a Digital Asset Risk and Incident Readiness Register to the unit head and the information security function
- Decide which cyber risks need new safeguards first, based on asset value and scored exposure
- Avoid prolonged outages and data loss caused by untested backups, missing patches and unclear incident reporting
- Coach colleagues on reporting suspicious events and following the unit's incident handling steps

Conclusion:

Back at work, the participant presents the Digital Asset Risk and Incident Readiness Register to the unit head and the information security function. They use it to agree which safeguards to fund or strengthen, who owns each asset and how incidents are reported and escalated. After the first incident drill or real event, the unit should update risk scores, record what slowed containment or recovery, and confirm that backup restores and access reviews were completed as planned.

Frequently Asked Questions FAQ:

What should participants know before a cyber risk management and digital asset protection course?

Participants should know the main systems, data and suppliers their unit relies on. Bringing a list of key applications, any existing asset or risk register and a recent incident or near miss makes the case work relevant to their own unit.

How does a cyber risk management and digital asset protection course differ from a board-level cyber governance course?

A board-level governance course helps directors set risk appetite and oversee cyber programmes. This course works at unit level, building an asset inventory, scoring risks, checking essential safeguards and practising incident handling steps that managers and staff carry out themselves.

Which essential controls support cyber risk management and digital asset protection?

CIS Controls v8.1 Implementation Group 1 sets out essential cyber hygiene safeguards, such as asset inventory, secure configuration, access control, patching, backup and awareness. NIST CSF 2.0 groups such outcomes into Govern, Identify, Protect, Detect, Respond and Recover.

What do participants take back from a cyber risk management and digital asset protection course?

Participants take back a Digital Asset Risk and Incident Readiness Register listing assets, owners, classification, scored risks, selected safeguards and incident reporting contacts, plus checklists for access reviews, backups and patching and a lessons learned log template.