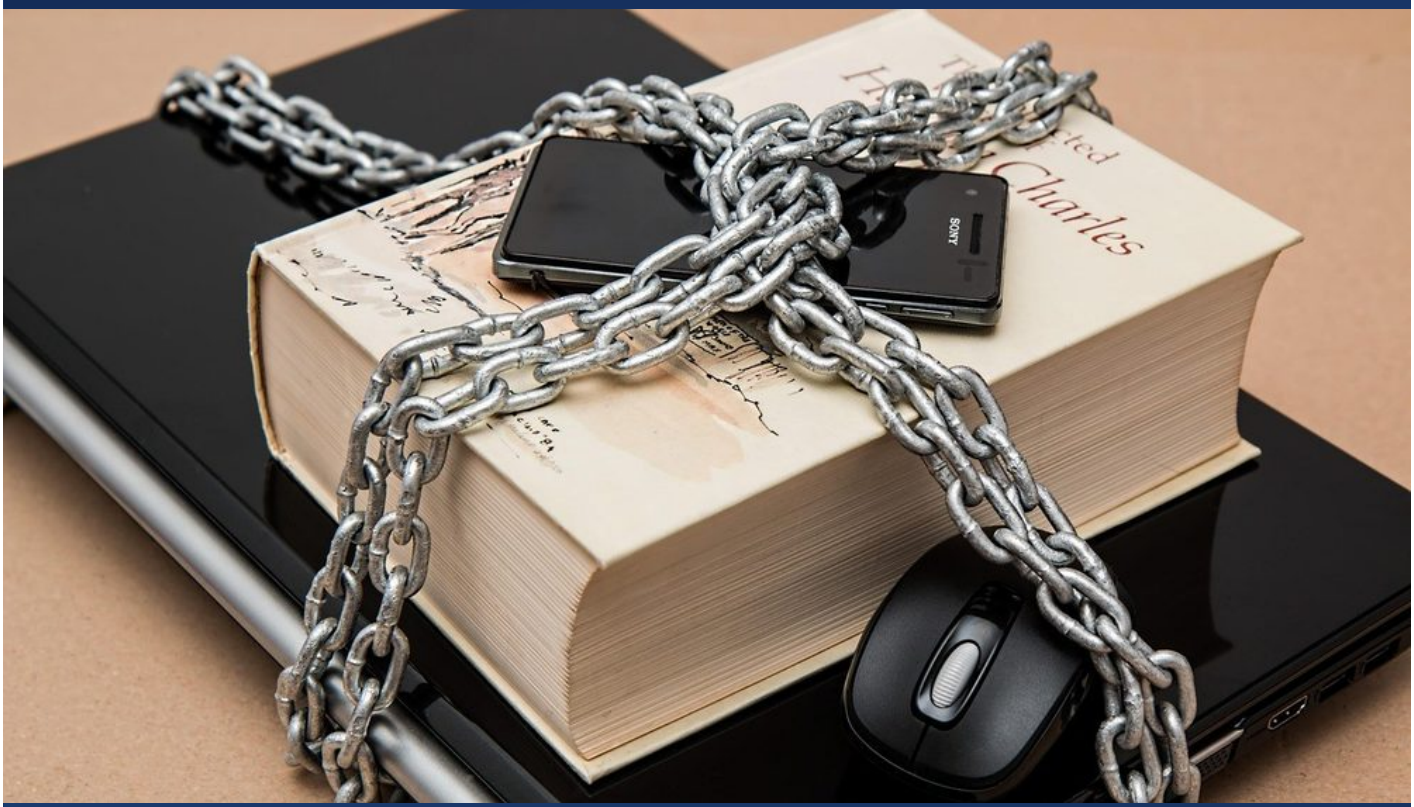
LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27001BNK — Information Security in Banking

ISO Certification Programme



LAPT — London Academy of Professional Training

Address 85 Great Portland Street, W1W 7LT, London, United Kingdom

Email info@lapt.org

Telephone +44 7513 283044

Web lapt.org

Reference MGT-BNK-27001BNK • ISO Management & Services

UKPRN 10067351 • Registered in England and Wales, company 4984798

6	30	180	430	60%	Lifetime
SUBJECTS	CHAPTERS	CLASSES	TOTAL MARKS	PASS MARK	VALIDITY

AT A GLANCE

REFERENCE	**MGT-BNK-27001BNK**
AWARD	**Certificate**
ASSESSMENT	**430 marks — 258 to pass (60%)**
PREREQUISITES	**None**
VALIDITY	**Lifetime**
AWARDING BODY	**LAPT — London Academy of Professional Training**

CURRICULUM

1 Compliance and Regulatory Issues

5 chapters · 30 classes · **65 marks**

• 1 Understanding Regulatory Frameworks in Banking — 6 classes

- › 1.1 Define Regulatory Frameworks in Banking
- › 1.2 Identify Key Regulatory Bodies and Their Roles
- › 1.3 Explain the Importance of Compliance in Banking Operations
- › 1.4 Analyze Common Regulatory Challenges Faced by Banks
- › 1.5 Evaluate the Impact of Regulatory Changes on Banking Practices
- › 1.6 Develop a Compliance Strategy for Regulatory Adherence

• 2 ISO 27001 Principles and Compliance — 6 classes

- › 2.1 Understand the Core Principles of ISO 27001
- › 2.2 Identify Key Compliance Requirements in Banking
- › 2.3 Analyze the Role of Risk Assessment in Information Security
- › 2.4 Explore the Structure of ISO 27001 Documentation
- › 2.5 Review Best Practices for Implementing ISO 27001
- › 2.6 Develop an Action Plan for Compliance in Your Organization

• 3 Risk Assessment and Management Strategies — 6 classes

- › 3.1 Identify Key Components of Risk Assessment in Banking
- › 3.2 Analyze Regulatory Requirements Influencing Risk Management
- › 3.3 Evaluate Common Risk Assessment Frameworks and Models
- › 3.4 Develop Risk Management Strategies for Banking Operations
- › 3.5 Implement Risk Mitigation Techniques in Compliance Practices
- › 3.6 Create a Risk Management Action Plan for Banking Leadership

• 4 Data Protection Regulations and Practices — 6 classes

- › 4.1 Understand Key Data Protection Regulations Affecting Banking
- › 4.2 Identify the Principles of Data Protection Compliance
- › 4.3 Analyze the Impact of GDPR on Banking Practices
- › 4.4 Evaluate Data Protection Risk Management Strategies
- › 4.5 Implement Best Practices for Data Handling in Banking
- › 4.6 Assess Data Breach Response Procedures in Banking Context

• 5 Developing a Compliance Culture in Banking Institutions — 6 classes

- › 5.1 Assessing Current Compliance Culture in Banking
- › 5.2 Identifying Key Compliance Risks in Financial Operations
- › 5.3 Developing Effective Communication Strategies for Compliance
- › 5.4 Engaging Leadership: Promoting a Culture of Accountability
- › 5.5 Implementing Training Programs to Foster Compliance Awareness
- › 5.6 Evaluating the Impact of Compliance Initiatives on Organizational Culture

2 Incident Response Management

5 chapters · 30 classes **65 marks**

- **1 Understanding Incident Response in Banking Contexts** — 6 classes
  - 1.1 Define Incident Response in Banking Contexts
  - 1.2 Identify Types of Security Incidents in Banking
  - 1.3 Explore the Incident Response Life Cycle
  - 1.4 Assess Roles and Responsibilities in Incident Management
  - 1.5 Analyze Case Studies of Banking Incident Responses
  - 1.6 Develop an Incident Response Plan Template for Banks
- **2 The Incident Response Lifecycle: Phases and Activities** — 6 classes
  - 2.1 Define the Incident Response Lifecycle
  - 2.2 Identify the Phases of Incident Response
  - 2.3 Explore Key Activities within Each Phase
  - 2.4 Establish Roles and Responsibilities in Incident Response
  - 2.5 Develop Effective Communication Strategies During Incidents
  - 2.6 Apply the Incident Response Cycle to Real-world Scenarios
- **3 Developing an Incident Response Plan Tailored to Banking Operations** — 6 classes
  - 3.1 Assess Current Security Posture for Incident Response
  - 3.2 Identify Key Stakeholders for Incident Management in Banking
  - 3.3 Define Roles and Responsibilities in Incident Response Teams
  - 3.4 Develop Incident Classification and Prioritization Criteria
  - 3.5 Create Communication Plans for Effective Incident Reporting
  - 3.6 Test and Revise the Incident Response Plan Through Simulations
- **4 Incident Detection and Threat Intelligence in Banking** — 6 classes
  - 4.1 Identify Methods for Detecting Security Incidents in Banking
  - 4.2 Analyze the Role of Threat Intelligence in Financial Institutions
  - 4.3 Evaluate Tools for Real-time Monitoring and Detection
  - 4.4 Develop a Threat Intelligence Sharing Protocol
  - 4.5 Create Incident Detection Criteria for Banking Operations
  - 4.6 Apply Threat Intelligence to Strengthen Incident Response Plans
- **5 Post-Incident Analysis and Continuous Improvement** — 6 classes
  - 5.1 Evaluate Incident Response Effectiveness
  - 5.2 Identify Root Causes of Security Incidents
  - 5.3 Document Findings and Lessons Learned
  - 5.4 Develop Actionable Improvement Recommendations
  - 5.5 Implement Changes to Incident Response Protocols
  - 5.6 Monitor and Review Continuous Improvement Measures

3 Information Security Governance

5 chapters · 30 classes **85 marks**

- **1 Foundations of Information Security in Banking** — 6 classes
  - 1.1 Define Key Concepts in Information Security for Banking
  - 1.2 Identify Regulatory Frameworks Impacting Information Security
  - 1.3 Analyze Common Risks and Threats in Banking Information Systems
  - 1.4 Explore the Role of Leadership in Enhancing Information Security
  - 1.5 Assess Best Practices for Information Security Governance
  - 1.6 Develop an Action Plan for Implementing Security Measures in Banking
- **2 Risk Management Frameworks in Banking** — 6 classes
  - 2.1 Identify Key Components of Risk Management Frameworks in Banking
  - 2.2 Analyze Regulatory Requirements Affecting Risk Management in Banking
  - 2.3 Evaluate Risk Assessment Methodologies Used in Banking
  - 2.4 Develop a Risk Management Strategy for Banking Institutions
  - 2.5 Implement Risk Mitigation Techniques in Banking Operations
  - 2.6 Review and Enhance the Effectiveness of Risk Management Practices
- **3 Developing an Information Security Governance Structure** — 6 classes
  - 3.1 Identify Key Components of an Information Security Governance Structure
  - 3.2 Assess Current Information Security Policies and Practices
  - 3.3 Establish Roles and Responsibilities in Information Security Governance
  - 3.4 Develop a Risk Management Framework for Information Security
  - 3.5 Create a Communication Plan for Information Security Policies
  - 3.6 Evaluate and Improve the Information Security Governance Framework
- **4 Compliance and Legal Considerations in Information Security** — 6 classes
  - 4.1 Identify Key Regulatory Frameworks for Information Security in Banking
  - 4.2 Analyze the Impact of GDPR on Banking Information Security Practices
  - 4.3 Evaluate the Role of Compliance Officers in Information Security Governance
  - 4.4 Assess Legal Obligations and Risks in Information Security Management
  - 4.5 Develop Strategies for Ensuring Compliance with Information Security Regulations
  - 4.6 Implement Best Practices for Legal and Regulatory Compliance in Banking
- **5 Continuous Improvement and Incident Management in Banking Security** — 6 classes
  - 5.1 Analyze Current Incident Management Procedures in Banking
  - 5.2 Identify Key Areas for Continuous Improvement in Security Measures
  - 5.3 Develop a Framework for Measuring Security Incident Responses
  - 5.4 Evaluate the Role of Leadership in Driving Security Improvements
  - 5.5 Implement Strategies for Training Staff on Incident Management Protocols
  - 5.6 Create an Action Plan for Enhancing Banking Security Based on Findings

4 ISO 27001 Implementation

5 chapters · 30 classes **65 marks**

- **1 Understanding ISO 27001 and Its Importance in Banking** — 6 classes
  - 1.1 Define ISO 27001 and Its Core Principles
  - 1.2 Explore the Relevance of Information Security in Banking
  - 1.3 Identify Key Components of the ISO 27001 Framework
  - 1.4 Analyze the Benefits of ISO 27001 Certification for Banks
  - 1.5 Assess Common Challenges in Implementing ISO 27001
  - 1.6 Develop a Roadmap for ISO 27001 Adoption in Banking Institutions
- **2 Key Components of ISO 27001: Policies and Frameworks** — 6 classes
  - 2.1 Identify Key Policies in ISO 27001
  - 2.2 Outline the ISO 27001 Framework Components
  - 2.3 Analyze the Role of Risk Assessment in Policy Development
  - 2.4 Develop Security Policies Aligned with ISO 27001 Standards
  - 2.5 Implement Monitoring and Review Processes for Policies
  - 2.6 Evaluate the Effectiveness of Information Security Frameworks
- **3 Risk Assessment and Management in Banking Security** — 6 classes
  - 3.1 Identify Key Risks in Banking Security
  - 3.2 Analyze Threats and Vulnerabilities in Financial Operations
  - 3.3 Evaluate Impact and Likelihood of Security Risks
  - 3.4 Develop Risk Mitigation Strategies for Banking
  - 3.5 Implement Risk Management Frameworks in Banking Institutions
  - 3.6 Monitor and Review Risk Management Processes in Banking
- **4 Implementing Information Security Controls and Procedures** — 6 classes
  - 4.1 Identify Key Information Security Risks in Banking
  - 4.2 Establish Information Security Policies and Procedures
  - 4.3 Define Roles and Responsibilities for Information Security
  - 4.4 Implement Technical Controls for Data Protection
  - 4.5 Conduct Security Awareness Training for Employees
  - 4.6 Monitor and Review Information Security Controls Effectively
- **5 Auditing and Continuous Improvement of ISO 27001 Compliance** — 6 classes
  - 5.1 Analyze the ISO 27001 Auditing Process
  - 5.2 Identify Key Audit Objectives and Criteria
  - 5.3 Evaluate Audit Findings and Recommendations
  - 5.4 Implement Corrective Actions for Non-Conformities
  - 5.5 Develop a Continuous Improvement Plan for Compliance
  - 5.6 Foster a Culture of Security Awareness and Monitoring

5 Leadership and Security Culture

5 chapters · 30 classes **85 marks**

- **1 Understanding Leadership Roles in Information Security** — 6 classes
  - 1.1 Define Leadership's Role in Information Security
  - 1.2 Identify Key Responsibilities of Security Leaders
  - 1.3 Analyze the Impact of Leadership on Security Culture
  - 1.4 Explore Effective Communication Strategies for Security Leaders
  - 1.5 Evaluate Leadership Styles and Their Influence on Security Practices
  - 1.6 Develop Actionable Plans to Strengthen Security Leadership
- **2 Developing a Security-Centric Leadership Strategy** — 6 classes
  - 2.1 Assess Current Leadership Practices for Security Integration
  - 2.2 Identify Key Elements of a Security-Centric Leadership Strategy
  - 2.3 Develop Objectives for Enhancing Security Culture in Leadership
  - 2.4 Create Action Plans for Implementing Security Leadership Strategies
  - 2.5 Evaluate Impact of Security-Centric Leadership on Organizational Culture
  - 2.6 Foster Continuous Improvement in Security Leadership Practices
- **3 Cultivating a Security Culture among Employees** — 6 classes
  - 3.1 Define and Understand Security Culture in Banking
  - 3.2 Identify Key Components of a Positive Security Culture
  - 3.3 Assess Current Security Attitudes Among Employees
  - 3.4 Develop Strategies to Improve Employee Engagement in Security
  - 3.5 Implement Training Programs to Foster Security Awareness
  - 3.6 Evaluate the Effectiveness of Security Culture Initiatives
- **4 Measuring and Enhancing Security Culture Efficacy** — 6 classes
  - 4.1 Define and Assess Key Elements of Security Culture
  - 4.2 Identify Metrics for Measuring Security Culture Efficacy
  - 4.3 Analyze Quantitative Data to Evaluate Security Practices
  - 4.4 Conduct Qualitative Surveys to Gather Employee Insights
  - 4.5 Develop Strategies to Enhance Security Culture Based on Findings
  - 4.6 Implement and Monitor Improved Security Practices in Banking
- **5 Leadership's Role in Crisis Management and Incident Response** — 6 classes
  - 5.1 Identify Leadership Responsibilities in Crisis Management
  - 5.2 Analyze the Impact of Leadership on Incident Response
  - 5.3 Develop Effective Communication Strategies for Leaders
  - 5.4 Evaluate Leadership Styles in Crisis Situations
  - 5.5 Foster a Security Culture During Crises
  - 5.6 Create Action Plans for Leadership in Incident Scenarios

6 Risk Management in Banking

5 chapters · 30 classes **65 marks**

- **1 Foundations of Risk Management in Banking** — 6 classes
  - 1.1 Define Key Concepts in Risk Management
  - 1.2 Identify Risk Types Specific to Banking
  - 1.3 Assess the Impact of Risks on Banking Operations
  - 1.4 Explore Regulatory Frameworks for Risk Management
  - 1.5 Implement Risk Mitigation Strategies in Banking
  - 1.6 Evaluate the Effectiveness of Risk Management Practices
- **2 Risk Identification and Assessment Techniques** — 6 classes
  - 2.1 Explore Key Concepts of Risk Management in Banking
  - 2.2 Identify Common Types of Risks in Banking Operations
  - 2.3 Analyze Risk Identification Techniques in Practice
  - 2.4 Assess Qualitative vs Quantitative Risk Assessment Methods
  - 2.5 Implement Risk Assessment Frameworks for Banking
  - 2.6 Evaluate Risk Assessment Case Studies in Banking Scenarios
- **3 Risk Mitigation Strategies and Best Practices** — 6 classes
  - 3.1 Identify Common Risks in Banking Operations
  - 3.2 Analyze Risk Assessment Techniques for Financial Institutions
  - 3.3 Develop Effective Risk Mitigation Plans
  - 3.4 Implement Best Practices for Data Security in Banking
  - 3.5 Evaluate the Effectiveness of Risk Mitigation Strategies
  - 3.6 Create a Continuous Improvement Plan for Risk Management
- **4 Regulatory Frameworks and Compliance in Risk Management** — 6 classes
  - 4.1 Identify Key Regulatory Frameworks in Banking
  - 4.2 Analyze the Role of Compliance in Risk Management
  - 4.3 Evaluate the Impact of Regulatory Changes on Banking Practices
  - 4.4 Assess Risk Management Strategies in Relation to Compliance
  - 4.5 Develop Practical Compliance Procedures for Risk Management
  - 4.6 Implement an Effective Compliance Monitoring System
- **5 Integrating Risk Management into Banking Operations** — 6 classes
  - 5.1 Assessing Current Risk Management Practices in Banking Operations
  - 5.2 Identifying Key Risks in Banking Operations
  - 5.3 Developing a Risk Management Framework for Banking
  - 5.4 Integrating Risk Management into Daily Banking Activities
  - 5.5 Evaluating the Effectiveness of Risk Management Strategies
  - 5.6 Communicating Risk Management Protocols to Banking Staff