LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27799 — Health Informatics Information Security Management

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 HL-HIT-27799 • ISO Health

UKPRN 10067351 • Registered in England and Wales, company 4984798

6	45	294	430	60%	Lifetime
SUBJECTS	CHAPTERS	CLASSES	TOTAL MARKS	PASS MARK	VALIDITY

AT A GLANCE

REFERENCE	**HL-HIT-27799**
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 Ethics in Health Informatics

10 chapters · 60 classes **65 marks**

- **1 Fundamentals of Health Informatics Compliance** — 6 classes
  - 1.1 Define Key Terms in Health Informatics Compliance
  - 1.2 Identify Legal Frameworks Governing Health Informatics
  - 1.3 Explore Ethical Principles in Health Informatics
  - 1.4 Analyze Compliance Challenges in Health Informatics
  - 1.5 Examine Case Studies of Health Informatics Non-Compliance
  - 1.6 Develop a Personal Action Plan for Ethical Compliance in Health Informatics
- **1 Understanding Ethical Principles in Health Informatics** — 6 classes
  - 1.1 Define Key Ethical Principles in Health Informatics
  - 1.2 Explore the Importance of Patient Consent in Data Handling
  - 1.3 Analyze Case Studies on Ethical Dilemmas in Health Informatics
  - 1.4 Assess the Role of Confidentiality in Health Informatics
  - 1.5 Evaluate Strategies for Ethical Decision-Making in Health Informatics
  - 1.6 Create an Ethical Framework for Managing Health Data
- **2 Ethical Considerations in Health Data Management** — 6 classes
  - 2.1 Identify Ethical Principles in Health Data Management
  - 2.2 Analyze Case Studies of Ethical Violations in Health Informatics
  - 2.3 Discuss the Role of Consent in Health Data Usage
  - 2.4 Evaluate Privacy Regulations Impacting Health Data Practices
  - 2.5 Develop Strategies for Ethical Decision-Making in Health Informatics
  - 2.6 Implement Compliance Checklists for Ethical Health Data Management
- **2 Legal Frameworks Governing Health Information Management** — 6 classes
  - 2.1 Identify Key Legal Frameworks in Health Information Management
  - 2.2 Analyze the Role of Data Protection Legislation in Health Informatics
  - 2.3 Examine Ethical Considerations in Patient Data Handling
  - 2.4 Discuss the Impact of GDPR on Health Information Practices
  - 2.5 Evaluate Compliance Requirements for Health Information Security
  - 2.6 Apply Legal and Ethical Principles to Real-World Health Informatics Scenarios
- **3 Risk Assessment and Management in Health Informatics** — 6 classes
  - 3.1 Identify Key Risks in Health Informatics
  - 3.2 Evaluate the Impact of Identified Risks on Patient Safety
  - 3.3 Analyze Regulatory Requirements for Health Data Security
  - 3.4 Develop a Risk Management Framework for Health Informatics
  - 3.5 Implement Mitigation Strategies for Identified Risks
  - 3.6 Monitor and Review Risk Management Practices in Health Informatics
- **3 Risk Management and Compliance in Health IT Systems** — 6 classes
  - 3.1 Identify Key Components of Risk Management in Health IT
  - 3.2 Analyze Compliance Requirements in Health Informatics
  - 3.3 Assess Potential Risks Associated with Health IT Systems
  - 3.4 Develop Risk Mitigation Strategies for Health IT Compliance
  - 3.5 Evaluate the Role of Leadership in Health IT Risk Management
  - 3.6 Formulate an Action Plan for Health Informatics Compliance Audits
- **4 Implementing Compliance Frameworks in Health IT** — 6 classes
  - 4.1 Identify Key Components of Compliance Frameworks in Health IT
  - 4.2 Analyze Regulatory Requirements Affecting Health Informatics
  - 4.3 Evaluate Existing Compliance Programs in Health Organizations
  - 4.4 Develop a Custom Compliance Framework for Health IT
  - 4.5 Implement Monitoring and Reporting Mechanisms for Compliance
  - 4.6 Promote a Culture of Compliance and Ethics in Health Informatics
- **4 Building a Culture of Ethics within Health Informatics Teams** — 6 classes
  - 4.1 Define Ethical Principles in Health Informatics
  - 4.2 Identify Ethical Dilemmas in Health Informatics Practice
  - 4.3 Assess the Impact of Ethics on Patient Care and Data Security
  - 4.4 Develop Strategies for Communicating Ethical Standards to Teams
  - 4.5 Create a Framework for Reporting Ethical Concerns in Health Informatics
  - 4.6 Evaluate Case Studies to Enhance Ethical Decision-Making Skills
- **5 Monitoring and Auditing for Compliance in Health Informatics** — 6 classes
  - 5.1 Identify Key Compliance Standards in Health Informatics
  - 5.2 Understand the Role of Auditing in Health Information Security
  - 5.3 Analyze Techniques for Effective Monitoring of Compliance
  - 5.4 Apply Risk Assessment Methods in Health Informatics Audits
  - 5.5 Evaluate Case Studies of Compliance Breaches and Their Implications
  - 5.6 Develop an Action Plan for Auditing and Monitoring Compliance
- **5 Responding to Ethical Dilemmas and Compliance Violations** — 6 classes
  - 5.1 Identify Ethical Dilemmas in Health Informatics
  - 5.2 Analyze Compliance Violations in Health Institutions
  - 5.3 Evaluate the Impact of Ethical Decisions on Patient Care
  - 5.4 Develop Strategies for Ethical Decision-Making
  - 5.5 Create a Compliance Violation Reporting Framework
  - 5.6 Implement Ethical Guidelines in Health Informatics Practices

2 Developing Security Policies

10 chapters · 60 classes **65 marks**

- **1 Understanding Health Informatics Security Frameworks** — 6 classes
  - 1.1 Define Key Concepts of Health Informatics Security
  - 1.2 Explore the Importance of Security Frameworks in Healthcare
  - 1.3 Identify Major Standards and Regulations Impacting Health Informatics Security
  - 1.4 Analyze Existing Health Informatics Security Frameworks
  - 1.5 Develop a Draft Security Policy Framework for Health Informatics
  - 1.6 Evaluate the Effectiveness of Security Policies in Health Informatics
- **1 Understanding the Context of Health Informatics Security Policies** — 6 classes
  - 1.1 Define the Essential Components of Health Informatics Security Policies
  - 1.2 Analyze the Role of Legislation in Shaping Security Policies
  - 1.3 Identify Stakeholders in Health Informatics Security Management
  - 1.4 Assess Risks and Vulnerabilities in Health Information Systems
  - 1.5 Develop Strategies for Effective Policy Communication
  - 1.6 Evaluate the Impact of Security Policies on Health Information Practice
- **2 Risk Assessment Methodologies in Health IT** — 6 classes
  - 2.1 Identify Key Risk Factors in Health IT Systems
  - 2.2 Analyze Different Risk Assessment Methodologies
  - 2.3 Evaluate the Impact of Risks on Health Informatics
  - 2.4 Prioritize Risks Using a Risk Matrix
  - 2.5 Develop Mitigation Strategies for Identified Risks
  - 2.6 Create a Risk Assessment Report for Health IT Stakeholders
- **2 Identifying Key Components of Effective Security Policies** — 6 classes
  - 2.1 Define Key Security Policy Objectives
  - 2.2 Analyze Current Security Threats and Vulnerabilities
  - 2.3 Identify Stakeholders in Security Policy Development
  - 2.4 Develop Essential Security Policy Components
  - 2.5 Evaluate Best Practices for Security Policy Implementation
  - 2.6 Create a Framework for Continuous Policy Review and Improvement
- **3 Crafting Effective Security Policies for Health Organizations** — 6 classes
  - 3.1 Analyze Existing Security Policies in Health Organizations
  - 3.2 Identify Key Components of an Effective Security Policy
  - 3.3 Formulate Security Objectives Tailored to Health Informatics
  - 3.4 Develop a Framework for Policy Implementation and Monitoring
  - 3.5 Create Training Strategies to Communicate Security Policies
  - 3.6 Evaluate and Revise Security Policies Based on Feedback
- **3 Frameworks and Standards for Health Informatics Security Policies** — 6 classes
  - 3.1 Identify Key Frameworks for Health Informatics Security
  - 3.2 Analyze Existing Standards in Health Informatics
  - 3.3 Evaluate Regulatory Requirements for Information Security
  - 3.4 Develop Comprehensive Security Policies Based on Frameworks
  - 3.5 Integrate Risk Management Strategies into Security Policies
  - 3.6 Implement Security Policies and Measure Effectiveness
- **4 Implementation Strategies for Security Policies** — 6 classes
  - 4.1 Assess Current Security Policies and Practices
  - 4.2 Identify Key Stakeholders for Policy Implementation
  - 4.3 Develop Actionable Steps for Policy Deployment
  - 4.4 Create Training Materials for Staff Engagement
  - 4.5 Establish Monitoring and Evaluation Metrics
  - 4.6 Conduct a Review and Revise Implementation Strategies
- **4 Risk Assessment and Management in Security Policy Development** — 6 classes
  - 4.1 Identify Key Risks in Health Informatics Security
  - 4.2 Analyze Impact and Likelihood of Identified Risks
  - 4.3 Evaluate Current Security Measures Against Risks
  - 4.4 Develop Risk Mitigation Strategies for Health Informatics
  - 4.5 Create a Risk Assessment Report for Stakeholders
  - 4.6 Implement Monitoring and Review Processes for Risk Management
- **5 Monitoring and Evaluating Security Policy Effectiveness** — 6 classes
  - 5.1 Define Key Performance Indicators for Security Policies
  - 5.2 Establish Methods for Data Collection and Monitoring
  - 5.3 Analyze Collected Data to Assess Policy Effectiveness
  - 5.4 Identify Gaps and Areas for Improvement in Policies
  - 5.5 Develop a Feedback Mechanism for Stakeholder Engagement
  - 5.6 Create a Reporting Framework for Policy Evaluation Findings
- **5 Implementation and Communication of Security Policies** — 6 classes
  - 5.1 Identify Key Components of Security Policies
  - 5.2 Analyze the Importance of Stakeholder Communication
  - 5.3 Develop a Plan for Policy Implementation
  - 5.4 Create Effective Training Materials for Staff
  - 5.5 Evaluate Methods for Monitoring Policy Compliance
  - 5.6 Revise and Update Security Policies Based on Feedback

3 Information Security Principles

5 chapters · 36 classes **85 marks**

- **1 Fundamentals of Information Security in Health Informatics** — 6 classes
  - 1.1 Understand the Importance of Information Security in Health Informatics
  - 1.2 Identify Key Concepts and Terminologies in Information Security
  - 1.3 Explore Common Threats and Vulnerabilities in Health Information Systems
  - 1.4 Analyze Legal and Ethical Considerations in Health Data Security
  - 1.5 Develop Strategies for Implementing Security Measures in Health Informatics
  - 1.6 Evaluate the Effectiveness of Information Security Policies in Healthcare Settings
- **2 Risk Management and Assessment in Healthcare Settings** — 6 classes
  - 2.1 Identify Key Risks in Healthcare Information Security
  - 2.2 Assess Vulnerabilities in Health Informatics Systems
  - 2.3 Evaluate Impact of Risks on Patient Safety and Privacy
  - 2.4 Prioritize Risks Based on Likelihood and Consequence
  - 2.5 Develop Mitigation Strategies for Identified Risks
  - 2.6 Implement Continuous Monitoring for Risk Management Effectiveness
- **3 Regulatory Compliance and Ethical Considerations** — 6 classes
  - 3.1 Identify Key Regulatory Frameworks Impacting Health Informatics
  - 3.2 Analyze Ethical Considerations in Health Information Security
  - 3.3 Evaluate Compliance Standards for Health Data Protection
  - 3.4 Implement Best Practices for Ethical Data Handling
  - 3.5 Assess Organizational Policies for Regulatory Compliance
  - 3.6 Develop a Compliance and Ethics Action Plan for Health Informatics
- **4 Implementing Security Controls in Health IT Systems** — 12 classes
  - 4.1 Identify Key Security Vulnerabilities in Health IT Systems
  - 4.1 Identify Key Security Controls for Health IT Systems
  - 4.2 Assess Risk Factors and Impacts on Patient Data Security
  - 4.2 Assess Vulnerabilities in Health Informatics Environments
  - 4.3 Explore Types of Security Controls for Health Informatics
  - 4.3 Develop a Risk Management Strategy for Health IT
  - 4.4 Develop a Comprehensive Security Control Implementation Plan
  - 4.4 Implement Technical Security Controls in Health IT Systems
  - 4.5 Monitor and Evaluate the Effectiveness of Security Controls
  - 4.5 Establish Policies for Data Access and User Authentication
  - 4.6 Train Staff on Best Practices for Security in Health IT Environments
  - 4.6 Evaluate the Effectiveness of Security Controls in Practice
- **5 Incident Response and Continuous Improvement** — 6 classes
  - 5.1 Identify Key Components of Incident Response Plans
  - 5.2 Analyze Real-World Case Studies of Security Incidents
  - 5.3 Develop a Step-by-Step Incident Response Procedure
  - 5.4 Formulate Effective Communication Strategies During Incidents
  - 5.5 Evaluate the Effectiveness of Incident Response Efforts
  - 5.6 Implement Feedback Loops for Continuous Improvement in Security

4 ISO 27799 Standards

5 chapters · 48 classes **65 marks**

• 1 Overview of ISO 27799 and Its Importance in Health Informatics — 12 classes

- 1.1 Define ISO 27799 and Its Key Components
- 1.1 Define ISO 27799 and Its Role in Health Informatics
- 1.2 Explore the Historical Context of ISO 27799 in Health Informatics
- 1.2 Explain the Core Principles of ISO 27799 Standards
- 1.3 Identify the Principles of Information Security Management in Health Informatics
- 1.3 Identify Key Components of Information Security Management
- 1.4 Discuss the Importance of Compliance with ISO 27799 Standards
- 1.4 Discuss the Importance of ISO 27799 for Patient Data Protection
- 1.5 Analyze Case Studies Illustrating the Impact of ISO 27799 Implementation
- 1.5 Evaluate the Impact of ISO 27799 on Health Organizations
- 1.6 Develop an Action Plan for Aligning Health Informatics Practices with ISO 27799
- 1.6 Apply ISO 27799 Standards to Develop a Health Informatics Security Plan

• 2 Risk Management Frameworks for Health Information Security — 6 classes

- 2.1 Define Key Concepts in Risk Management Frameworks
- 2.2 Identify Components of ISO 27799 Risk Management
- 2.3 Analyze Risk Assessment Methodologies in Health Informatics
- 2.4 Evaluate Existing Security Controls and Their Effectiveness
- 2.5 Develop a Risk Register for Health Information Security
- 2.6 Create an Action Plan for Implementing Risk Management Strategies

• 3 Implementing Information Security Policies in Health Organizations — 12 classes

- 3.1 Understand the Importance of Information Security in Health Organizations
- 3.1 Define Information Security Policies in Health Organizations
- 3.2 Analyze Key Components of ISO 27799 Standards
- 3.2 Identify Key Components of ISO 27799 Standards
- 3.3 Identify Potential Information Security Risks in Health Environments
- 3.3 Analyze Risk Management Practices in Health Informatics
- 3.4 Develop Comprehensive Information Security Policies
- 3.4 Develop Effective Communication Strategies for Policy Implementation
- 3.5 Implement Training Programs for Staff on Security Policies
- 3.5 Evaluate Compliance and Monitoring Techniques for Health Organizations
- 3.6 Evaluate and Monitor the Effectiveness of Security Policies
- 3.6 Create an Action Plan for Policy Enforcement and Training

• 4 Monitoring and Measuring Health Informatics Security Controls — 6 classes

- 4.1 Define Key Performance Indicators for Health Informatics Security
- 4.2 Establish Baseline Metrics for Security Controls
- 4.3 Implement Monitoring Tools for Data Protection Compliance
- 4.4 Conduct Regular Audits of Security Measures in Health Informatics
- 4.5 Analyze Security Incident Reports to Improve Controls
- 4.6 Develop Action Plans Based on Monitoring Results and Stakeholder Feedback

• 5 Future Trends in Health Information Security and ISO 27799 Adaptations — 12 classes

- 5.1 Explore Emerging Technologies in Health Information Security
- 5.1 Analyze Emerging Threats to Health Information Security
- 5.2 Analyze Current Challenges in Implementing ISO 27799
- 5.2 Evaluate the Impact of Technology on ISO 27799 Standards
- 5.3 Evaluate the Impact of Data Privacy Regulations on ISO 27799
- 5.3 Explore Best Practices for Implementing ISO 27799 Adaptations
- 5.4 Discuss Future Trends Influencing Health Data Management
- 5.4 Assess the Role of Leadership in Health Informatics Compliance
- 5.5 Integrate ISO 27799 with Evolving Cybersecurity Practices
- 5.5 Develop Strategies for Future-Proofing Health Information Security
- 5.6 Develop Action Plans for Adapting to Future Security Standards
- 5.6 Propose Innovations to Enhance ISO 27799 Relevance

5 Leadership in Information Security

10 chapters · 60 classes **65 marks**

• 1 Understanding Health Informatics and Information Security — 6 classes

- 1.1 Define Health Informatics and Its Importance in Security
- 1.2 Explore Key Concepts of Information Security in Healthcare
- 1.3 Identify Common Threats and Vulnerabilities in Health Informatics
- 1.4 Analyze the Role of Leadership in Information Security Management
- 1.5 Develop Strategies for Effective Information Security Governance
- 1.6 Implement Best Practices for Enhancing Security in Health Informatics

• 1 Understanding the Role of Leadership in Health Information Security — 6 classes

- 1.1 Define Leadership Roles in Health Information Security
- 1.2 Identify Key Responsibilities of Health Information Security Leaders
- 1.3 Analyze Leadership Styles Impacting Information Security Culture
- 1.4 Explore Effective Communication Strategies for Security Leadership
- 1.5 Develop a Leadership Framework for Health Information Security
- 1.6 Create an Action Plan for Enhancing Leadership in Information Security

• 2 Regulatory and Ethical Standards in Health Information Security — 6 classes

- 2.1 Identify Key Regulatory Standards in Health Information Security
- 2.2 Analyze Ethical Considerations in Health Information Management
- 2.3 Evaluate the Impact of GDPR on Health Information Security Practices
- 2.4 Assess Compliance Requirements for Health Organizations
- 2.5 Develop a Framework for Ethical Decision-Making in Health Informatics
- 2.6 Implement Strategies to Enhance Leadership in Regulatory Compliance

• 2 Risk Management in Health Informatics: Leadership Perspectives — 6 classes

- 2.1 Identify Key Risks in Health Informatics
- 2.2 Assess the Impact of Information Security Breaches
- 2.3 Evaluate Risk Management Frameworks for Health Leadership
- 2.4 Develop Risk Mitigation Strategies in Health Informatics
- 2.5 Engage Stakeholders in Risk Management Discussions
- 2.6 Implement a Culture of Security Awareness in Health Organizations

• 3 Leadership Roles and Responsibilities in Information Security Management — 6 classes

- 3.1 Define Leadership Roles in Information Security Management
- 3.2 Identify Key Responsibilities of Information Security Leaders
- 3.3 Assess Leadership Styles Impacting Information Security Culture
- 3.4 Develop Communication Strategies for Security Leadership
- 3.5 Evaluate Decision-Making Processes in Information Security
- 3.6 Implement Leadership Best Practices for Security Governance

• 3 Developing Policies and Procedures for Information Security in Healthcare — 6 classes

- 3.1 Analyze Current Healthcare Information Security Needs
- 3.2 Identify Key Stakeholders in Policy Development
- 3.3 Design Framework for Information Security Policies
- 3.4 Develop Procedures for Incident Response and Reporting
- 3.5 Implement Training Strategies for Staff Compliance
- 3.6 Evaluate and Revise Policies for Continuous Improvement

• 4 Risk Assessment and Management Strategies for Health IT — 6 classes

- 4.1 Identify Key Risks in Health IT Environments
- 4.2 Analyze Impact and Likelihood of Information Security Risks
- 4.3 Develop a Risk Assessment Framework for Health Informatics
- 4.4 Implement Risk Management Strategies in Health IT Systems
- 4.5 Evaluate and Monitor Risk Management Effectiveness
- 4.6 Communicate Risk Assessment Findings to Stakeholders

• 4 Communication Strategies for Promoting Information Security Awareness — 6 classes

- 4.1 Identify Key Stakeholders in Information Security Communication
- 4.2 Develop Effective Messaging for Information Security Awareness
- 4.3 Utilize Visual Aids to Enhance Understanding of Security Policies
- 4.4 Implement Two-Way Communication Channels for Feedback
- 4.5 Assess the Impact of Communication Strategies on Security Awareness
- 4.6 Create an Action Plan for Ongoing Information Security Education

• 5 Developing an Effective Information Security Culture in Healthcare Organizations — 6 classes

- 5.1 Identify Key Components of an Information Security Culture in Healthcare
- 5.2 Assess Current Information Security Practices and Their Leadership Implications
- 5.3 Develop Strategies for Enhancing Employee Awareness of Security Protocols
- 5.4 Implement Leadership Techniques to Foster Open Communication about Security
- 5.5 Create an Action Plan for Regular Training and Security Drills in Healthcare Settings
- 5.6 Evaluate the Effectiveness of Security Culture Initiatives within Your Organization

• 5 Evaluating Information Security Programs: The Leader's Role — 6 classes

- 5.1 Assessing Current Information Security Practices
- 5.2 Identifying Key Metrics for Security Evaluation
- 5.3 Analyzing Risks and Vulnerabilities in Security Programs
- 5.4 Engaging Stakeholders in Security Program Evaluation
- 5.5 Implementing Continuous Improvement in Security Practices
- 5.6 Communicating Evaluation Outcomes to the Organization

6 Risk Assessment in Health IT

5 chapters · 30 classes **85 marks**

- **1 Foundations of Risk Assessment in Health IT** — 6 classes
  - 1.1 Define Key Concepts in Risk Assessment for Health IT
  - 1.2 Identify Types of Risks in Health Informatics
  - 1.3 Analyze the Impact of Data Breaches in Healthcare
  - 1.4 Evaluate Existing Risk Assessment Frameworks in Health IT
  - 1.5 Develop a Risk Assessment Strategy for Health Information Systems
  - 1.6 Create an Action Plan for Mitigating Identified Risks in Health IT
- **2 Identifying Health IT Risks and Vulnerabilities** — 6 classes
  - 2.1 Define Health IT Risks and Vulnerabilities
  - 2.2 Identify Common Vulnerabilities in Health IT Systems
  - 2.3 Assess the Impact of Vulnerabilities on Patient Data
  - 2.4 Evaluate Existing Risk Assessment Frameworks in Health IT
  - 2.5 Develop a Risk Identification Checklist for Health IT
  - 2.6 Propose Mitigation Strategies for Identified Risks
- **3 Risk Analysis Techniques in Health Informatics** — 6 classes
  - 3.1 Define Risk Assessment in Health Informatics
  - 3.2 Identify Common Risk Analysis Techniques
  - 3.3 Evaluate the Benefits of Qualitative vs Quantitative Risk Analysis
  - 3.4 Conduct a Basic Risk Assessment Case Study
  - 3.5 Develop Mitigation Strategies Based on Risk Analysis Findings
  - 3.6 Present and Communicate Risk Assessment Results Effectively
- **4 Developing Risk Mitigation Strategies for Health IT** — 6 classes
  - 4.1 Identify Key Risks in Health IT Systems
  - 4.2 Analyze Impact and Likelihood of Identified Risks
  - 4.3 Explore Risk Mitigation Frameworks for Health IT
  - 4.4 Develop Targeted Mitigation Strategies for Specific Risks
  - 4.5 Evaluate the Effectiveness of Mitigation Strategies
  - 4.6 Communicate Risk Mitigation Plans to Stakeholders
- **5 Continuous Monitoring and Improvement of Risk Management Practices** — 6 classes
  - 5.1 Evaluate Current Risk Management Practices in Health IT
  - 5.2 Identify Key Metrics for Continuous Monitoring of Risks
  - 5.3 Implement Tools for Effective Risk Assessment
  - 5.4 Analyze Data for Improving Risk Management Strategies
  - 5.5 Develop an Action Plan for Ongoing Risk Mitigation
  - 5.6 Review and Revise Risk Management Processes for Sustainability