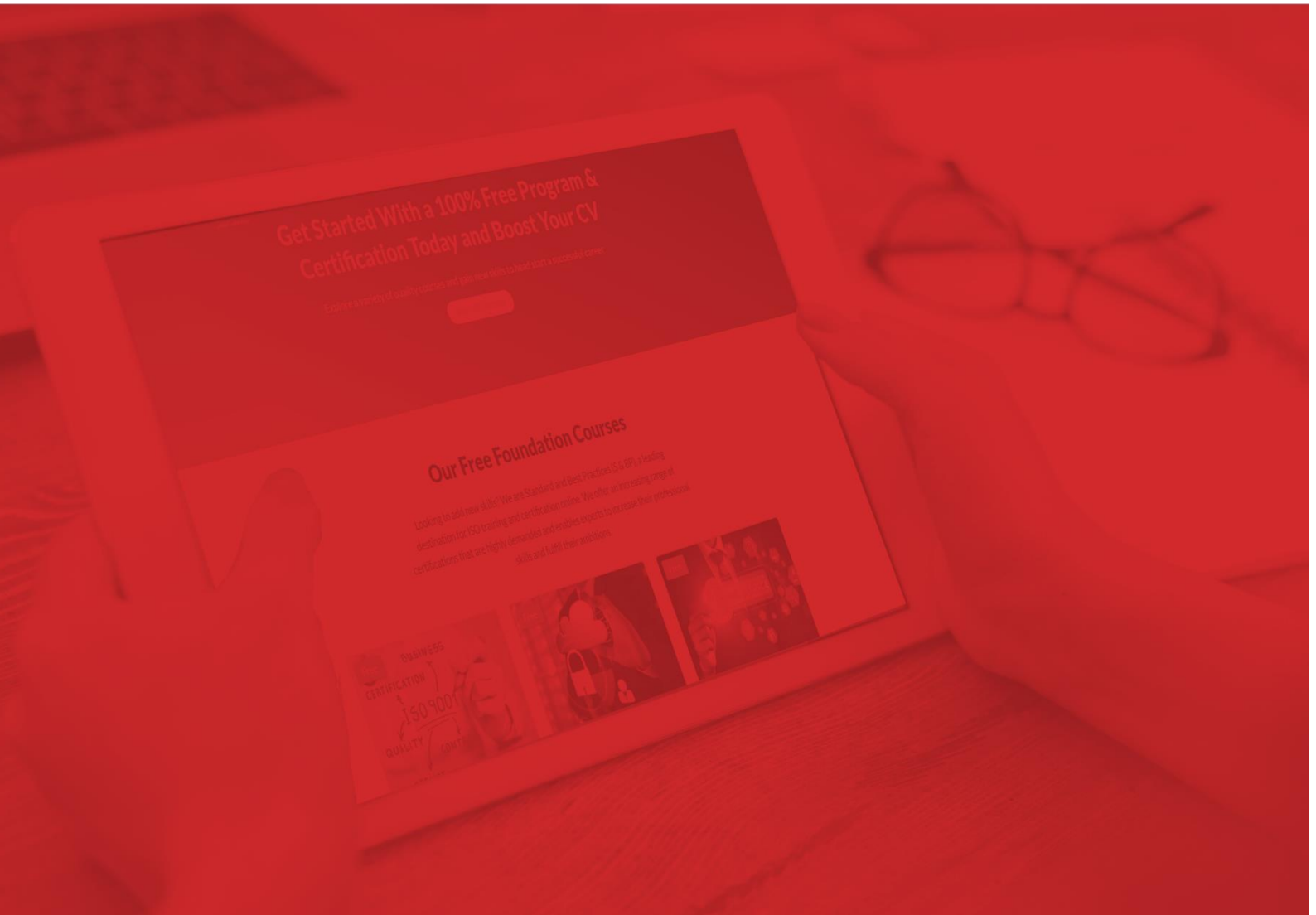
...global validation

SBP ISO/IEC 27005:2022 (ISRM) MANAGER COURSE- CASE STUDIES



ISO/IEC 27005:2022 (ISRM) MANAGER COURSE CASE STUDIES

CASE STUDY #1

Case Study: Implementing the Risk Management Framework (RMF) in a Federal Agency

Background

The Federal Agency for Health and Safety (FAHS) is a U.S. government agency responsible for ensuring public health and safety. Recently, FAHS has faced increased scrutiny over the protection of sensitive health data, including personally identifiable information (PII) of citizens. In response, the agency has decided to implement the Risk Management Framework (RMF) to enhance its information security and privacy practices.

Case Study Overview

The FAHS is preparing to execute the RMF, which involves seven key steps. The agency must integrate information security and privacy requirements in accordance with OMB Circular A-130, ensuring a comprehensive approach to managing security and privacy risks.

1. Prepare to Execute the RMF

Objective: Establish context and priorities for managing security and privacy risks.

Actions:

- **Establish Context:** FAHS conducts a series of workshops with key stakeholders to identify critical assets and define risk tolerance levels. They focus on health data systems and their impact on public health.
- **Priorities:** The agency prioritizes protecting PII and ensuring compliance with federal privacy regulations. They outline the importance of maintaining the confidentiality, integrity, and availability of health data.

Outcome: FAHS creates a risk management strategy document outlining the priorities and context for managing risks. This document serves as a foundational guide for the subsequent RMF steps.

2. Categorize the System

Objective: Categorize the system and information processed based on the impact of loss.

Actions:

- **System Categorization:** FAHS categorizes its health information systems into three levels: high, moderate, and low impact. Systems handling PII are categorized as high impact due to the potential consequences of data breaches.
- **Impact Analysis:** The agency conducts an impact analysis to understand the potential effects of data loss or compromise on public health and safety.

Outcome: FAHS produces a system categorization report detailing the impact levels of different systems and the types of information processed. This report is used to guide the selection of appropriate controls.

3. Select and Tailor Controls

Objective: Select an initial set of controls and tailor them to reduce risk.

Actions:

- **Control Selection:** FAHS selects controls from ISO/IEC 27001:2022, Annex A, and other relevant sources such as sector-specific codes of practice. For high-impact systems, controls include encryption, access controls, and audit logging.
- **Tailoring Controls:** The agency tailors the selected controls to address specific risks identified in the previous step. For instance, additional encryption measures are implemented for PII processing systems.

Outcome: FAHS develops a tailored controls catalog that specifies the controls required for each system, including detailed descriptions of how these controls will be implemented.

4. Implement Controls

Objective: Implement the controls and describe their deployment.

Actions:

- **Control Implementation:** FAHS deploys the selected controls, such as installing encryption software, configuring access controls, and setting up audit logging systems. They also train staff on the new security measures.
- **Documentation:** The agency documents the implementation process, including the configuration of controls and the roles responsible for their management.

Outcome: FAHS produces an implementation report detailing how each control is employed within the system and its environment of operation.

5. Assess Controls

Objective: Assess whether the controls are implemented correctly, operating as intended, and meeting requirements.

Actions:

- **Control Assessment:** FAHS conducts an internal audit and vulnerability assessment to verify the effectiveness of the controls. They review audit logs, test encryption protocols, and assess access control mechanisms.
- **Feedback:** The agency gathers feedback from system users and administrators to identify any issues or areas for improvement.

Outcome: FAHS generates an assessment report that includes findings on the effectiveness of the controls, any identified issues, and recommendations for improvements.

6. Authorize the System

Objective: Authorize the system based on an acceptable risk determination.

Actions:

- **Risk Authorization:** FAHS evaluates the risk to organizational operations, assets, and individuals. They prepare an authorization package that includes the risk assessment results, control implementation details, and the assessment report.
- **Approval:** The agency's senior management reviews the package and grants authorization for the system to operate, acknowledging the residual risks.

Outcome: FAHS receives formal authorization to operate the system, with documented approval from senior management.

7. Monitor the System

Objective: Continuously monitor the system and controls, including assessing effectiveness and documenting changes.

Actions:

- **Ongoing Monitoring:** FAHS implements a continuous monitoring program to regularly assess control effectiveness. They track changes to the system and its environment, perform periodic risk assessments, and update the risk management strategy as needed.
- **Reporting:** The agency prepares regular reports on the security and privacy posture of the system, highlighting any new risks or changes.

Outcome: FAHS establishes a robust monitoring process, including regular updates and reports to ensure ongoing compliance and effective risk management.

Integration of Information Security and Privacy

OMB Circular A-130 Requirements: FAHS integrates privacy controls into the RMF process to manage risks related to PII. They collaborate with both information security and privacy programs to address all relevant risks, including unauthorized access, data quality, and compliance with privacy regulations.

Privacy Controls:

- **Data Handling:** Implement privacy controls to ensure proper handling of PII, including access restrictions and data minimization practices.
- **Compliance:** Regularly review privacy policies and procedures to ensure compliance with applicable regulations and address any gaps.

Outcome: FAHS successfully integrates privacy into the RMF process, ensuring that both information security and privacy objectives are met.

Conclusion

By following the RMF steps, FAHS has enhanced its approach to managing information security and privacy risks. The agency's comprehensive implementation of the RMF ensures that it effectively protects sensitive health data while complying with federal regulations and maintaining public trust.

CASE STUDY #2

Case Study: Establishing Context for Information Security Risk Management at TechNet Solutions

Background:

TechNet Solutions, a mid-sized IT service provider, specializes in developing and maintaining custom software solutions for clients in various industries, including finance, healthcare, and e-commerce. The company operates across three regions: North America, Europe, and Asia. Due to the nature of its business, TechNet handles sensitive customer data such as personally identifiable information (PII), payment details, and healthcare records. As the company expanded, so did the complexity of its operations and its exposure to information security risks.

Recognizing the need for a more formalized approach to managing these risks, TechNet Solutions decided to implement an Information Security Management System (ISMS) based on **ISO/IEC 27001:2022**. In this case study, we explore how TechNet established the organizational context as part of their ISMS, specifically focusing on **Module 5: Context Establishment**.

ISO/IEC 27005:2022 (ISRM) MANAGER COURSE CASE STUDIES

1. Organizational Considerations

Scenario:

TechNet Solutions is comprised of multiple departments including IT operations, research and development, and customer support. Each department has its own responsibilities, but they all share the common objective of ensuring the confidentiality, integrity, and availability of information. As TechNet operates in regulated sectors like finance and healthcare, the organization's risk appetite is low, especially when it comes to handling sensitive data.

The company's leadership team has assigned the Chief Information Officer (CIO) as the **Risk Owner**, responsible for overseeing risk management activities. Each department head is also designated as a sub-risk owner for their respective operational areas, with accountability for managing specific risks tied to their activities.

Key Considerations:

- **Size and Complexity:** TechNet is a medium-sized company but operates in multiple sectors, each with its own regulatory requirements. This necessitates a diverse risk management approach.
- **Sector Requirements:** TechNet's presence in heavily regulated sectors like finance and healthcare means the company must comply with numerous standards and regulations, significantly lowering its risk appetite.
- **Risk Appetite:** Due to the sensitive nature of its operations, TechNet has adopted a conservative approach to risk, accepting only minimal risk exposure in areas that might affect customer data or operational stability.

Outcome:

The organization clearly defined the role of risk owners and established a framework for managing information security risks across departments. Each department head is accountable for the risks within their domain and regularly reports to the CIO, who consolidates this information for top management.

2. Identifying Basic Requirements of Interested Parties

Scenario:

As part of the context establishment, TechNet Solutions identified its key **interested parties**, which included customers, regulatory bodies (e.g., HIPAA, GDPR authorities), employees, business partners, and contractors. Each party has its own expectations and requirements regarding information security.

For example:

- **Customers** expect their sensitive data to be protected, especially in compliance with regulatory standards like GDPR for European clients or HIPAA for healthcare data.
- **Regulators** require strict adherence to industry-specific regulations and standards such as PCI-DSS for financial transactions and HIPAA for healthcare information.
- **Internal Employees** expect secure access to systems and protection of internal resources from cyber threats.

To meet these expectations, TechNet identified several **reference documents** to define their security rules:

- **ISO/IEC 27001:2022** for the ISMS framework.
- **ISO 27799** for managing healthcare information.
- **NIST SP 800-53** for additional security controls, particularly for financial services.
- **GDPR compliance guidelines** for handling data from European clients.
- **Internal security policies** and **contractual obligations** with partners, including cloud service providers.

Outcome:

TechNet systematically identified the requirements of interested parties and incorporated these into their ISMS, ensuring that all relevant standards, laws, and contractual obligations were addressed in their risk management activities.

3. Applying Risk Assessment

Scenario:

TechNet conducts a variety of risk assessments based on the different operational processes, including:

- **Project Management:** Risk assessments are embedded into project initiation phases, particularly for client projects involving sensitive data.
- **Vulnerability Management:** Regular risk assessments are performed on identified vulnerabilities, ensuring timely patching and remediation.
- **Incident Management:** Risks are reassessed post-incident to prevent future occurrences of similar events.

An example occurred when a **third-party vendor** responsible for cloud storage faced a data breach. TechNet initiated an impromptu risk assessment to evaluate the potential impact on its customers' data. The assessment revealed that while the vendor had solid encryption practices, a **gap** existed in TechNet's own data backup strategy.

Outcome:

The risk assessment led to enhanced controls over third-party vendor management and an improved internal backup strategy. These measures significantly reduced the likelihood of future data breaches and ensured that TechNet could recover from incidents with minimal data loss.

4. Establishing and Maintaining Information Security Risk Criteria

Scenario:

TechNet defined its risk criteria based on several considerations:

- **Uncertainties:** Cyber-attacks, third-party vendor failures, and insider threats.
- **Consequence and Likelihood:** Consequences were measured in terms of financial losses, operational downtime, and damage to reputation, while likelihood was predicted based on past incidents and industry trends.
- **Risk Evaluation:** TechNet established specific thresholds for risk acceptance. For example, any risk that could result in more than a **1% loss of annual revenue** was deemed unacceptable and required immediate mitigation.

Risk acceptance levels were aligned with TechNet's overall risk appetite. For instance, while minor system outages due to internal updates were considered acceptable, any event leading to **customer data leakage** was strictly unacceptable.

Outcome:

By setting clear risk criteria, TechNet ensured consistency in evaluating risks across its different departments. This helped streamline decision-making, particularly during **risk treatment** and resource allocation.

5. Risk Acceptance Criteria

Scenario:

TechNet had to decide on its **risk acceptance criteria** for different risk categories:

- **Regulatory Non-Compliance Risks:** These risks were classified as **high** with near-zero tolerance, given the severe penalties associated with GDPR and HIPAA violations.
- **Operational Risks:** For risks like minor downtime in non-critical systems, TechNet established a higher acceptance threshold, as these risks were deemed manageable with existing controls.
- **Financial Risks:** A cost/benefit analysis helped establish criteria for accepting risks that could result in minor financial losses but were outweighed by the cost of additional controls.

For example, TechNet accepted the risk of occasional system slowdowns during off-peak hours, as the cost of upgrading infrastructure outweighed the potential impact on customer experience.

Outcome:

Risk acceptance criteria provided TechNet's management with a structured approach to make informed decisions. Different risk levels were assigned to different management tiers, allowing the **IT department** to handle low-level operational risks, while **top management** focused on strategic risks.

6. Criteria for Performing Information Security Risk Assessments

Scenario:

TechNet developed a standard approach for risk assessments that focused on three key aspects:

- **Consequences:** Loss of confidentiality, integrity, or availability of critical customer data was considered the highest impact scenario, particularly for healthcare and financial clients.
- **Likelihood:** Past data breaches in the industry were considered when predicting the likelihood of cyber-attacks.
- **Level of Risk:** A combination of consequence and likelihood was used to assess the overall risk, with high-risk areas prioritized for treatment.

For example, while the risk of a **major cyber-attack** was assessed as low likelihood, the **consequence** was deemed so severe that it warranted significant investment in **advanced threat detection technologies**.

Outcome:

By applying these criteria consistently, TechNet could effectively prioritize its resources and focus on managing risks that posed the greatest threat to its objectives.

Conclusion:

Through a systematic approach to **context establishment**, TechNet Solutions was able to align its ISMS with the company's strategic objectives. By clearly identifying risk owners, understanding the requirements of interested parties, and setting risk assessment and acceptance criteria, TechNet established a robust framework for managing information security risks. This case study highlights the importance of context in building an effective ISMS and the real-world impact of these activities on an organization's risk posture.

CASE STUDY #3

Case Study: Information Security Risk Treatment Process

Overview:

XYZ Corporation, a global technology service provider, handles sensitive customer data across multiple regions, providing cloud services to thousands of organizations. The company adheres to the ISO/IEC 27001:2022 framework to manage its Information Security Management System (ISMS). Due to recent increases in cyberattacks on cloud service providers, XYZ Corporation conducted a risk assessment and identified several critical risks that could compromise the confidentiality, integrity, and availability of its services.

The company now needs to develop a **Risk Treatment Plan** based on the results of this risk assessment. The aim is to reduce risks to an acceptable level by implementing a combination of preventive, detective, and corrective controls. This case study outlines the treatment process for three of the prioritized risks.

1. Risk: Unauthorized Access to Customer Data

Risk Description:

Due to improper access controls on cloud storage systems, there is a potential for unauthorized access to sensitive customer data. If exploited, this risk could lead to a significant data breach, resulting in customer trust loss, legal penalties, and financial damage.

Risk Treatment Options:

- **Modify the risk** by strengthening access controls.

Control Selection Process:

The team determines controls from **ISO/IEC 27001:2022 Annex A**, specifically focusing on the control sets related to access management and encryption. Based on the risk, the following controls were deemed necessary:

- **Access Control (A.9)**: Implement multi-factor authentication (MFA) and role-based access control (RBAC) to restrict access to sensitive data only to authorized users.
- **Cryptographic Controls (A.10)**: Encrypt customer data both in transit and at rest to protect confidentiality, even in the event of unauthorized access.

Control Implementation:

- **MFA Implementation**: A documented process to roll out MFA for all administrators accessing the cloud storage system. Ownership is assigned to the IT Security Manager, who will monitor the implementation through access logs. Weekly reports will be sent to the Chief Information Officer (CIO).
- **RBAC**: Roles are defined within the HR system, with necessary access rights mapped. The IT department enforces this through Active Directory policies, ensuring only authorized personnel can access sensitive data.

Control Effectiveness:

The controls reduce the **likelihood** of unauthorized access significantly by enforcing stricter access protocols. However, these preventive measures are supplemented by detective and corrective controls.

2. Risk: Malware Infection Through External Vendors

Risk Description:

XYZ Corporation uses third-party software vendors to maintain critical systems. The risk assessment revealed that one vendor had lax security controls, creating a potential entry point for malware that could disrupt services.

Risk Treatment Options:

- **Share the risk** by requiring the vendor to adhere to XYZ's security standards and implement additional security measures.

Control Selection Process:

The necessary controls are selected from **ISO/IEC 27001:2022** and **ISO/IEC 27017** (cloud security). A combination of preventive, detective, and corrective controls is identified:

- **Supplier Security Policy (A.15)**: Ensure that the vendor implements mandatory security policies, including anti-malware solutions and frequent patch updates.
- **Security Incident Management (A.16)**: Introduce real-time monitoring of external connections to detect any malicious activity early.
- **Audit and Compliance (A.18)**: Conduct regular third-party audits to verify the security posture of external vendors.

Control Implementation:

- **Vendor Agreement**: A contract addendum is signed with the vendor, stipulating mandatory malware protection measures and regular security reviews.

- **Real-Time Monitoring**: XYZ's IT Security team sets up Intrusion Detection Systems (IDS) on all vendor-facing endpoints. This system will alert the team if any suspicious activity is detected.

Control Effectiveness:

The real-time monitoring **detects** any malware attempts early, while third-party audits ensure the vendor's **compliance** with security standards, effectively mitigating the risk.

3. Risk: Loss of Data Due to Physical Theft of Laptops

Risk Description:

Several employees at XYZ Corporation use company-issued laptops to work remotely. The risk assessment highlighted that the loss or theft of laptops could lead to the exposure of sensitive customer and company information.

Risk Treatment Options:

- **Modify the risk** by enhancing physical security measures and implementing data encryption on all devices.

Control Selection Process:

Based on the identified risks, the necessary controls are chosen from **ISO/IEC 27001:2022 Annex A**:

- **Mobile Device Management (MDM)**: Introduce a solution that can remotely wipe the data from any stolen device.
- **Data Encryption (A.10)**: Encrypt all sensitive data stored on the laptops to prevent unauthorized access if a device is lost or stolen.

Control Implementation:

- **MDM Solution**: A remote device management platform is rolled out across all company laptops. The IT team is responsible for initiating remote wipes if any device is reported missing. Ownership is assigned to the Operations Manager.
- **Data Encryption**: All laptops are configured with encryption software that automatically encrypts stored data. IT security will perform periodic checks to ensure that encryption is active on all devices.

Control Effectiveness:

While encryption reduces the **consequences** of data exposure from stolen laptops, the MDM solution adds an additional layer of security, enabling the company to erase sensitive information before it can be accessed by malicious actors.

Determining Control Necessity:

Special attention was paid to determining whether each selected control was necessary:

- **Effect on Risk Likelihood or Consequence**: Each control was evaluated based on how it affects the likelihood or consequence of each risk. For example, data encryption was deemed necessary to reduce the consequences of laptop theft.
- **Preventive, Detective, and Corrective Mix**: The selected controls form a resilient risk treatment plan by combining preventive measures (such as MFA and encryption), detective controls (such as IDS), and corrective controls (such as remote wipe capabilities).

Outcome:

After implementing the controls, XYZ Corporation was able to modify its information security risks to a level that met the organization's risk criteria for acceptance. The ISMS compliance was maintained, and the company continued to monitor and improve its risk treatment plans through periodic reviews and audits.

Lessons Learned:

1. **Tailored Controls**: The effectiveness of the risk treatment process depends on tailoring the selected controls to the specific risks faced by the organization.
2. **Balance of Costs and Benefits**: A careful balance was maintained between the cost of implementing the controls and the potential impact of untreated risks. This was especially evident when deciding between adding or removing redundant controls.
3. **Continuous Monitoring and Improvement**: The controls were not static. They were regularly reviewed to ensure they were operating effectively, especially as new risks emerged and as the organization evolved.

This case study demonstrates a real-world application of the **Information Security Risk Treatment Process** and highlights the importance of a structured, methodical approach to managing information security risks.

ISO/IEC 27005:2022 (ISRM) MANAGER COURSE CASE STUDIES

CASE STUDY #4

Context:
ABC Corporation, a multinational financial services company, handles sensitive personal, financial, and operational data across its global operations. The company has implemented an Information Security Management System (ISMS) in accordance with **ISO/IEC 27001:2022** to ensure the protection of its assets, data integrity, and customer trust. Due to the dynamic nature of cybersecurity threats and organizational changes, ABC Corporation regularly performs information security risk assessments and risk treatment processes as part of its overall operational activities.

Section 8.1 - Performing Information Security Risk Assessment Process

Background:

ABC Corporation is undergoing a digital transformation that involves migrating several legacy systems to a cloud infrastructure, incorporating new third-party vendors, and implementing customer-facing mobile applications. These changes, along with the constantly evolving cybersecurity threat landscape, prompted the need for an **Information Security Risk Assessment**. According to **ISO/IEC 27001:2022, Clause 6.1**, risk assessments must be carried out at planned intervals or when significant events occur.

Inputs:

- **Risk Assessment Criteria**: Documents outlining the organization's criteria for evaluating information security risks.
- **Risk Acceptance Criteria**: Internal documents detailing the acceptable levels of residual risk for the organization.
- **Change Documentation**: Details on the system migration to the cloud and vendor integration.

Triggers:

1. The company's ongoing digital transformation and migration to a cloud platform, involving sensitive financial data.
2. Increased instances of ransomware attacks targeting financial institutions in the region.
3. Regulatory changes that require stricter data protection measures for financial services.

Risk Assessment Process:

The risk assessment was initiated due to these organizational and external factors. In alignment with **ISO/IEC 27001:2022, Clause 6.1.2 a)**, the company conducted a formal risk assessment

involving stakeholders from the IT department, compliance team, legal counsel, and business units affected by the migration.

Steps in the Risk Assessment Process:

1. **Asset Identification**: The assets affected by the migration were identified, including customer data, transaction records, and proprietary financial algorithms.
2. **Threat Identification**: The key threats were identified, including data breaches, system outages, malware attacks, and third-party vendor risks.
3. **Vulnerability Assessment**: Weaknesses in the company's current infrastructure, including inadequate encryption for data at rest in the legacy systems and weak access control policies in vendor systems, were assessed.
4. **Risk Evaluation**: Using the predefined risk criteria, each identified risk was rated based on its potential impact (high, medium, low) and the likelihood of occurrence (likely, unlikely, rare).
5. **Risk Acceptance Criteria**: Risks that exceeded the organization's tolerance levels were marked for treatment, while minor risks were accepted based on internal guidelines.

Outputs:

- **Evaluated Risks**: Risks related to unauthorized access during cloud migration, inadequate vendor security protocols, and vulnerabilities in the new mobile application were prioritized as high-impact risks.
- **Documented Information**: A risk assessment report was generated, including detailed descriptions of each risk, their impact, likelihood ratings, and decisions on whether each risk needed treatment or was acceptable.

Section 8.2 - Performing Information Security Risk Treatment Process

Background:

Following the risk assessment, several high-priority risks were identified that needed to be addressed through the **Information Security Risk Treatment Process**. As per **ISO/IEC 27001:2022, Clause 8**, the organization began formulating and implementing a risk treatment plan to reduce the identified risks to acceptable levels.

Inputs:

- **Evaluated Risks**: High-priority risks identified in the previous risk assessment process, including:
    - **Risk 1**: Unauthorized access to sensitive data during cloud migration.
    - **Risk 2**: Inadequate security measures at third-party vendor systems.
    - **Risk 3**: Vulnerabilities in the mobile application that could expose customer data to attackers.

Risk Treatment Options:

For each risk, the following risk treatment options were considered:

1. **Mitigate**: Implement security measures to reduce the risk likelihood or impact.
2. **Avoid**: Alter business activities to eliminate the risk.
3. **Transfer**: Outsource the risk to a third party, such as through cybersecurity insurance.
4. **Accept**: Acknowledge the risk without additional measures, as the residual risk is deemed acceptable.

Risk Treatment Process:

1. **Risk 1: Unauthorized Access During Cloud Migration**
    - **Treatment Plan**: Strengthen cloud security by encrypting data both at rest and in transit, and implementing multi-factor authentication (MFA) for all administrative access to the cloud environment.
    - **Implementation**:
        - The IT team encrypted all data before migration using advanced encryption standards (AES).
        - MFA was rolled out to all employees and contractors accessing the cloud systems.
        - A cloud security monitoring system was established to detect any unauthorized access attempts in real-time.
    - **Residual Risk**: After the controls were implemented, the residual risk was deemed acceptable, and ongoing monitoring was scheduled.
2. **Risk 2: Inadequate Security Measures at Third-Party Vendors**
    - **Treatment Plan**: Require vendors to adhere to ABC Corporation's security policies, conduct third-party audits, and integrate their systems with ABC's cybersecurity monitoring.
    - **Implementation**:
        - All vendors were required to sign new contractual agreements that mandated adherence to specific security standards, such as encryption and incident response protocols.
        - The company conducted security audits of vendor systems and assessed their compliance with the required security measures.
        - Vendor systems were integrated with ABC's monitoring system to detect any potential security breaches or policy violations.
    - **Residual Risk**: After ensuring compliance and integrating vendor systems into the security infrastructure, the residual risk was reduced to an acceptable level.
3. **Risk 3: Mobile Application Vulnerabilities**
    - **Treatment Plan**: Implement secure coding practices, conduct regular penetration testing, and employ mobile application security testing tools to identify and fix vulnerabilities.
    - **Implementation**:

- The development team applied secure coding principles to fix vulnerabilities in the application's authentication and encryption mechanisms.
- A third-party security firm was hired to perform penetration testing on the mobile application.
- Mobile security testing tools were deployed to regularly assess the application for new vulnerabilities as updates and new features were introduced.

- **Residual Risk**: After addressing critical vulnerabilities and establishing ongoing testing practices, the residual risk was considered manageable.

Triggers:

- **Digital Transformation**: The need to treat risks related to the migration of sensitive data to the cloud.
- **Regulatory Compliance**: Legal requirements for financial institutions to ensure the protection of customer data.
- **Vendor Management**: Concerns about third-party vendor security and its potential impact on ABC Corporation's overall security posture.

Outputs:

- **Residual Risks**: Risks associated with cloud migration, vendor management, and mobile application vulnerabilities were mitigated to an acceptable level based on the company's risk acceptance criteria.
- **Documented Risk Treatment Plan**: A comprehensive plan detailing the actions taken to mitigate each risk, with responsibility assigned to specific teams for ongoing management and review.

Implementation Guidance for Risk Assessment and Treatment:

The risk assessment and treatment processes outlined in **ISO/IEC 27001:2022, Clause 6.1 and Clause 8**, were integrated into ABC Corporation's operational activities. This integration was managed through periodic reviews and adjustments aligned with the company's **annual budget cycle** and **vendor procurement processes**. The company also ensured that risk assessments were scheduled in time for funding applications and were reassessed following the results of budget allocations.

The process of treating risks was dynamic, with regular evaluations of the evolving threat landscape. ABC Corporation understood that risk treatment is not a one-time action but an ongoing process that requires constant monitoring and reassessment.

Conclusion:

ISO/IEC 27005:2022 (ISRM) MANAGER COURSE CASE STUDIES

The case study of ABC Corporation highlights the practical application of **ISO/IEC 27001:2022** in performing information security risk assessments and treatments. The organization successfully managed its risks related to cloud migration, vendor security, and mobile application vulnerabilities by following a structured approach based on **ISO/IEC 27001's** guidelines. By integrating risk management into its day-to-day operations, ABC Corporation ensured that its information security risks were managed effectively, maintaining customer trust and regulatory compliance.