SECURITY MANAGEMENT (CW)

Module Code: KH6054CEM

Name: Shehab El Din Mohamed, ID: 202101590

EXECUTIVE SUMMARY:

This report outlines a cybersecurity risk assessment conducted for FinServCo to support ISO/IEC 27001 compliance. Six key risks were identified, including phishing threats, legacy system vulnerabilities, weak firewall infrastructure, and BYOD-related exposure. Most of the risks were rated **High** or **Extreme** and require immediate treatment.

Recommendations include system improvements, system improvements, heightened access control measures, advanced email protection, and improved backup and endpoint security policies. Also, the **Acceptable Use Policy** was revised to clarify its scope, responsibilities, and compliance.

Table of Contents

Table of Figures

1.INTRODUCTION:

FinServCo is an organization with multiple aspects in the field of financial services, having a significant employee base that works in handling sensitive customer and financial information. It has an information technology framework consisting of a centralized banking system, customer relationship management (CRM) system based on cloud, messaging and email service, along with multiple databases containing sensitive financial details. These systems are accessible through desktop as well as mobile devices inside the organization's premises as well as remote environments. Given the sensitive nature of the information and the applicable regulatory requirements specific to the financial services sector, FinServCo is undertaking a comprehensive cybersecurity risk assessment to comply with the **ISO/IEC 27001** standard. The **ISO/IEC 27001** standard is the international standard for Information Security Management Systems. Furthermore, this standard provides a structured approach to managing vulnerabilities in information security, protecting both the integrity and confidentiality of information to ensure business continuity.

This assessment seeks to examine the current threat landscape, assess the existing controls in place withing the organization, and verify compliance with current best practices and security standards in the industry such as the **ISO/IEC 27005** & **Nist 800-30** standards. Recommendations on strategic and operational improvements to strengthen the organization's cybersecurity posture will also be provided in this assessment to support its compliance with **ISO/IEC 27001**.

2.METHODOLOGY:

2.1 Frameworks Utilized

The risk assessment has been done using an amalgamation of internationally recognized frameworks ensuring systematic, structured, and standardized industry procedure:

- **ISO/IEC 27005**: Provides a framework of guidelines for information security risk management in support of **ISO/IEC 27001**. It defines the risk management process, Including context establishment, risk identification, analysis, evaluation, treatment, and continuous monitoring.

- **NIST SP 800-30**: Offers a comprehensive guide for performing risk assessments. It complements **ISO/IEC 27005** by providing a tactical, threat-driven model for identifying and analyzing information security risks.

These frameworks ensure both governance-level compliance and operational-level risk insight.

2.2 Risk Assessment Process

The risk assessment process follows the five key phases outlined in **ISO/IEC 27005,** Visualized below in the **ISO/IEC 27005** Risk Management Process model:

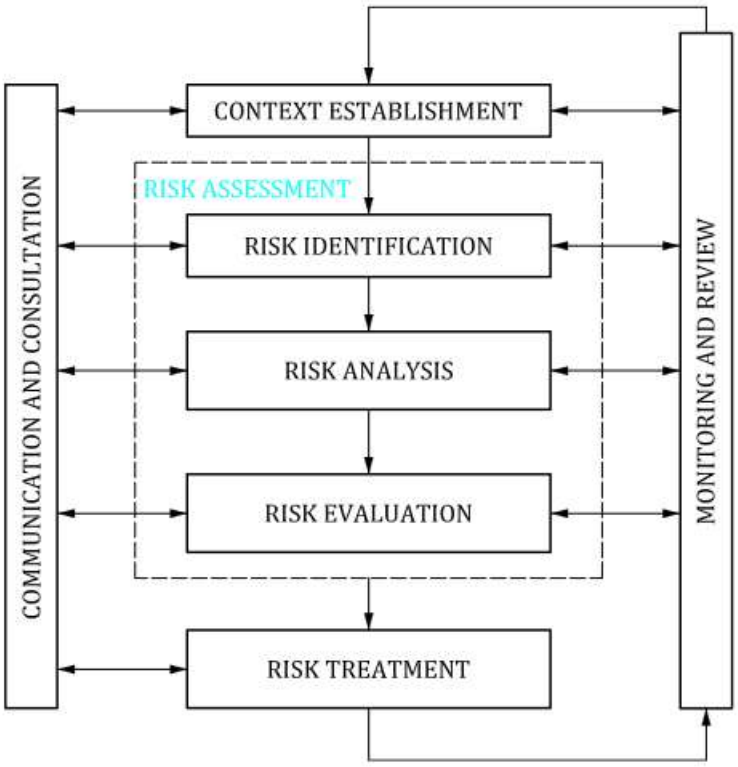

Figure 1: The risk management process

These five stages include:

1. Context Establishment: Defining the scope and risk acceptance relevant to FinServCo's information systems.

2. Risk Identification: Discovering potential threats, vulnerabilities, and impacted assets within the organization's infrastructure.

3. Risk Analysis: Determining the likelihood and impact of each identified risk to prioritize them effectively.

4. Risk Evaluation: Comparing the results of the risk analysis with the risk acceptance to identify the risks that require intervention.

5. Risk Treatment: Identifying appropriate controls and mitigation strategies to reduce unacceptable risks.

3.SCOPE & BOUNDARIES:

The assessment of information security vulnerabilities focuses on FinServCo's key information assets and sensitive data-processing infrastructure, handling financial data and sensitive customer information. This includes cloud-based architecture as well as in-house platforms used by workers stationed on-premises and remotely.

3.1 In-Scope Assets

- Core Banking System: A centralized system installed locally to perform transactional processes as well as account management. It is assumed that legacy components may still exist within this system.

- Customer Relationship Management (CRM): A cloud-based solution administered by FinServCo, with security configurations and access controls managed internally.

- Email and messaging services: Including Microsoft Exchange and Teams, accessible from desktops and mobile devices. Basic spam filtering is in place, but advanced threat detection is not fully deployed.

- Databases: Contain customer records, financial data, and audit logs. These are hosted within the internal network and are backed up regularly, though backups are assumed to reside in the same logical network segment.

- Employee Devices: Desktops, laptops, and mobile devices used across office and remote settings. Remote access is conducted via VPN with MFA, but Mobile Device Management (MDM) not uniformly enforced on BYOD devices.

- Network Infrastructure: Core networking equipment including firewalls, routers, and a VPN gateway supporting remote work. The firewalls in use are outdated and may no longer receive regular firmware updates or vendor support. Wi-Fi networks are segmented between employee and guest access.

4.RISK IDENTIFICATION:

The identification of the risks followed the methodology of the **ISO/IEC 27005** standard but focused on FinServCo's critical information assets, technology infrastructure, and operations. Identification was achieved through a thorough examination of the available system configurations, known vulnerabilities, and threat vectors.

Key resources used to identify risks included:

- Infrastructure documentation and architectural overview.
- Coordination with the relevant authorities and technical leads.

- Security control observations.
- Benchmarking against common threats in the financial services sector.

These risks include both external and internal threat vectors and cover a range of technical, procedural, and human vulnerabilities. All identified risks have been registered in a risk register and classified based on business impact, threat category, and affected assets. Figures 2,3, and 4 show the risk identification section inside the risk register.

This risk assessment is aligns with:		**CONTEXT** *(For Guidance, See Tab 3)*	**RISK IDENTIFICATION**			
RISK #	**CATEGORY**	**BUSINESS OBJECTIVE/ PRIORITY**	**RISK EVENT**	**RISK CAUSE**	**IMPACT**	**CURRENT TREATMENTS**
Add identifiers to better organize and track risks.	*Which category does this Risk Event fall under?*	*What business objective/priority does this Risk Event affect (e.g., Mandate letter, strategic directive, etc.)?*	*What events could impact the achievement of objectives (can be positive or negative)?*	*What Risk Cause (trigger, circumstance, uncertainty) could increase the Likelihood of the Risk Event occurring? There are usually multiple Risk Causes leading to a Risk Event.*	*How would the Risk Event **impact** the achievement of the objective/priority?*	*What Treatments are **currently** in place to manage the Risk Event? Focus on Treatments that either reduce the Likelihood (column H) of the Risk Event or can reduce the Consequence (column I) if the Risk Event occurs.*
R1(Core Banking System Risk)	Technical/ Infrastructure	Secure, uninterrupted banking operations	Unauthorized access via legacy components	Unpatched outdated software; Legacy modules	Data compromise, financial loss; regulatory breach	Firewall, role-based access, audit logs
R2 (CRM system)	Acess Control / Insider Threat	Protect customer data confidentiality and ensure authorized data access	Excessive internal user access to customer data	Misconfigured role-based access controls; lack of periodic access review	Exposure or misuse of customer data; potential regulatory violations (e.g., GDPR)	Access groups defined by department; admin access restricted to CRM admins; standard HR onboarding/ offboarding processes in place.

Figure 2: Risk Identification

R3 (Email & Messaging Platform)	Social Engineering / Email Security	Maintain secure communication channels and prevent unauthorized system access	Employees fall victim to phishing emails	Lack of advanced threat detection; inconsistent user awareness training	Compromise of user credentials, unauthorized access to systems, potential malware infection, or data breach	Basic spam filters in place; occasional security awareness emails; no centralized phishing detection system
R4 (Databases and Backup)	Malware / Data Availability	Ensure availability and recoverability of critical customer and financial data	Ransomware encrypts both production and backup databases	Backups are stored within the same network zone as active systems, making them susceptible to infection during a ransomware attack	Permanent data loss, extended operational downtime, regulatory non-compliance, customer trust damage	Regular backups performed; antivirus installed; no network segmentation between live data and backup storage

Figure 3: Risk Identification

R5 (Employee Devices (BYOD))	Endpoint Security / Mobile Device Management	Protect sensitive data across all access points and maintain endpoint compliance	Unauthorized access or data leakage from personal mobile devices	Lack of enforces Mobile Device Management (MDM) and inconsistent endpoint control on BYOD devices	Sensitive data could be leaked, lost, or accessed by unauthorized users; compliance issues may arise if regulatory data is compromised	VPN and MFA required for access; employee policy encourages secure device use, but enforcement is limited
R6(Network Infrastructure)	Network Security / Infrastructure	Prevent unauthorized access and protect perimeter network integrity	Intrusion through outdated firewalls	Firewalls are no longer supported by the vendor and lack modern intrusion detection capabilities or regular firmware updates	External attackers may bypass perimeter defenses, leading to system compromise, lateral movement within the network, and data breaches	Upgrading existing firewalls to Next-Generation Firewalls (NGFWs) that offer advances features / Ensure regular firmware updates

Figure 4: Risk Identification

5.RISK ANALYSIS:

The risks identified in FinServCo's environment are evaluated using the **ISO/IEC 27005** methodology. For each risk identified, an analysis was made on its likelihood of occurrence and the consequence it would have on business operations, customer data integrity, and compliance with regulatory requirements. Fig.5 shows the risk rating matrix used to analyze the risks identified. Figures 6, 7, and 8 show the risk ratings of each risk identified (1 - 6) inside the risk register.

Risk Rating Matrix

LIKELIHOOD

5	LOW	MED	HIGH	EXT	EXT
4	LOW	MED	HIGH	HIGH	EXT
3	LOW	MED	MED	HIGH	HIGH
2	LOW	LOW	MED	MED	MED
1	LOW	LOW	LOW	LOW	LOW
	1	2	3	4	5

CONSEQUENCE

LIKELIHOOD X CONSEQUENCE			
SCORE	0 – 5	=	LOW
SCORE	6 – 10	=	MEDIUM
SCORE	12 – 16	=	HIGH
SCORE	20 – 25	=	EXTREME

Figure 5: Risk Rating Matrix Table

ANALYSIS Residual risk rating with treatments in place *(For Guidance, See Tab 4)*			
L (1-5)	**C (1-5)**	**RISK RATING**	**HEAT MAP**
How likely?	*How severe?*	*(LxC)*	*Rating with current treatments in place*
4	*4*	16	***HIGH***
3	*2*	6	***MEDIUM***

Figure 6: Risk Rating

4	4	16	HIGH
4	5	20	EXTREME

Figure 7: Risk Rating

3	4	12	HIGH
4	4	16	HIGH

Figure 8: Risk Rating

5.1 Analysis of risks

The highest risk discovered is R4 (ransomware targeting backup data). Which is classified as Extreme due to the lack of segmentation between production and backup environments. If this vulnerability is exploited, it can lead to permanent data loss and substantial disruption of business operations. Recommended mitigation controls, such as immutable backups and cloud replication, are expected to reduce this risk to an acceptable level.

R1 (legacy system vulnerabilities) is another major concern. While the system operates behind firewalls with role-based access, outdated components present significant exposure. A system upgrade and decommissioning plan will help reduce this to a low residual risk.

Phishing attack (R3) were evaluated thoroughly because of the lack of advanced threat detection mechanisms and improper employee training. The implementation of a security gateway coupled with phishing simulation training should mitigate the threat; however, ongoing phishing will be a persistent threat.

R5 (BYOD exposure) and R6 (outdated firewalls) are infrastructure concerns. Lack of endpoint control, in addition to weak perimeter defenses, heightens the susceptibility of the organization to attacks. Remediation measures suggested will include the deployment of Mobile Device Management (MDM) systems for personal devices, and the substitution of outdated firewalls with Next-Generation Firewalls (NGFWs) with integrated threat detection.

R2 (excessive CRM access rights), while not as severe as the other, still poses a privacy and compliance risk. Role-based access policies and periodic user access reviews are expected to address this and reduce the risk to a low level.

6.RISK EVALUATION:

The evaluation involved mapping the results of the risk assessment against the predetermined risk acceptance criteria of FinServCo, developed based on the **ISO/IEC 27001** standard. The criteria specify the risks that are acceptable versus those requiring mitigation:

- **Low risks** may be accepted and monitored.
- **Medium risks** can be tolerated with regular oversight, depending on the context.
- **High and Extreme risks** are deemed unacceptable and require treatment.

Figures 9, 10, and 11 show the risk evaluation section inside the risk register. Based on the evaluation mentioned previously, all six identified risks exceed FinServCo's acceptable risk threshold in their current state, with four risks rated as high as (**High**) and one as (**Extreme**). Only the CRM access control was initially rated as (**Medium**), but due to its potential regulatory implications, it has also been marked for treatment. All risks have documented treatment plans that aim to reduce their severity to an acceptable residual level,

typically (**Medium**) or (**Low**), through a combination of technical controls, policy updates, and user awareness initiatives. Following these treatment plans ensure that FinServCo remains on track to meet the requirements of the ISO 27001 standard.

EVALUATION *(For Guidance, See Tab 5)*			TREATMENT MANAGEMENT					
ADEQUACY OF CURRENT TREATMENTS	ACTION	TREND	ADDITIONAL PLANNED TREATMENT	DELIVERABLES	TASK OWNER	DUE DATE	DEPENDENCIES/ INTER-RELATIONSHIPS	STATUS
Non-existent Inadequate Adequate Robust	*Will you do more to manage the risk (treat) or choose to accept and monitor?*	*If applicable, has this risk rating changed over time? Has column J increased (upward trend), decreased (downward trend) or not changed (static)*	*What Treatments are needed to **further** manage the Risk Event? Focus on Treatments that either reduce the Likelihood (column H) of the Risk Event or can reduce the Consequence (column I) if the Risk Event occurs.*	*Future Treatments will come in what form (e.g., a project plan, a briefing note, report, funding request, other)?*	*Who will take the lead on this mitigation?*	*When should the deliverable be ready? (Optional)*	*Do the Risk Event or Treatments depend on another team or organization? Do they impact another group?*	*On Track Slowed Stalled*
Inadequate	Treat	Static	Conduct a phased decomissioning of unsupported legacy modules and replace with secure, updated components.	Legacy system upgrade plan / Risk Remediation report / Compliance validation log	Legacy system upgrade plan: **Khaled Mostafa** / Risk remediation report: **Layla Fathy** / Compliance validation log: **Mohamed Hassan**	30/06/2025	Development team / Compliance Team	On Track
Adequate	Treat	Static	Implement a formal role-based access control (RBAC) policy for the CRM system. Perform periodic user access reviews and enforce the principle of least privilege. Remove or adjust excessive rights where applicable.	CRM role-based access policy document / Quarterly user access review process setup / User rights adjustment and remediation log	CRM role-based access policy document: **Layla Mahmoud** / Quarterly user access review process setup: **Mina Younes** / User rights adjustment and remediation log **Yasmeen Fawzy**	15/06/2025	HR Department	On Track

Figure 9: Risk Evaluation

Inadequate	Treat	Static	Deploy a cloud-based email security gateway with advanced anti-phishing, spoofing, and malware detection capabilities. Establish mandatory phishing awareness training for all employees, and simulate periodic phishing tests.	Implementation of email threat protection / Phishing awareness training program design / Launch of quarterly phishing simulation campaigns	Implementation of email threat protection system: **Ziad mohsen** / Phishing awareness training program design: Ahmed Nabil / Launch of quarterly phishing simulation campaigns: Ahmed Nabil	1/7/2025	IT Operations Team / HR Department	On Track
Inadequate	Treat	Static	Segment backup infrastructure from production systems. Implement immutable (read-only) backup storage with offsite or cloud-based replication. Perform periodic backup integrity testing.	Backup network segmentation plan and implementation / Deployment of immutable/cloud backup storage / Quarterly backup restoration testing report	Backup network segmentation plan and implementation: **Yousef Magdy** / Deployment of immutable/cloud backup storage: **Hana sherif** / Quarterly backup restoration testing report: **Omar Mohamed**	1/8/2025	Disaster Recovery Team / IT Infrastructure Team	On Track

Figure 10: Risk Evaluation

Inadequate	Treat	Static	Enforce organization-wide Mobile Device Management (MDM) policies for all devices accessing corporate data. Restrict access to sensitive resources on unmanaged devices. Deploy containerization for work apps and introduce mobile endpoint monitoring.	MDM solution deployment and onboarding plan / BYOD access policy and user communication rollout / Monitoring and enforcement dashboard setup	MDM solution deployment and onboarding plan: **Sarah Fathy** / BYOD access policy and user communication rollout: **Haitham Ahmed** / Monitoring and enforcement dashboard setup: **Ali Kamel**	15/07/2025	HR Department / Legal Department	On Track
Inadequate	Treat	Static	Replace legacy firewalls with Next-Generation Firewalls (NGFWs) featuring IPS, threat intelligence feeds, application-layer filtering, and logging.	Firewall upgrade procurement and deployment / Configuration of IPS and threat intelligence feeds	Firewall upgrade procurement and deployment: **Hala mahmoud** / Configuration of IPS and threat intelligence feeds: **Hosny mohamed**	30/07/2025	Procurement Team / Finance Department	On Track

Figure 11: Risk Evaluation

7.RECOMMENDATIONS:

Following the risk assessment, several recommendations are made to enhance FinServCo's cybersecurity framework and to reduce all the risks identified to acceptable levels based on **ISO 27001** standard.

7.1 Technical Measures

1. Upgrade legacy systems to close vulnerabilities within the core banking environment.
2. Implement Role-Based Access Control (RBAC) in the CRM system and conduct regular access reviews.
3. Deploy advanced email security solutions and launch phishing awareness training for employees.
4. Improve backup strategy by separating backup environments, enabling immutable backups, and testing restoration procedures.
5. Introduce Mobile Device Management (MDM) across employee-owned devices to secure endpoint access.
6. Replace outdated firewalls with Next-Generation Firewalls (NGFWs) and integrate them with centralized monitoring systems.

7.2 Policy Improvements (Acceptable Use Policy)

As part of the risk mitigation strategy, FinServCo's **Acceptable Use Policy was** revised. Key changes include:

- Addition of FinServCo's name in the heading for clearer authorship.
- Addition of new sections such as purpose, scope, definition & terms, and revision history to align with ISO 27001.
- Clearer language and structure regarding personal use, social media, and system monitoring.
- Stronger enforcement guidance and clearer reference to related security policies.

8.CONCLUSION:

The current risk assessment has determined the key cybersecurity risks that FinServCo is facing and has suggested specific mitigation strategies intended to reduce these risks to tolerable levels. Through the implementation of technical security measures, improving governance frameworks, and updating the **Acceptable Use Policy**, the organization will improve its general security posture, be compliant with **ISO 27001** requirements, and achieve better protection for its data, systems, and business processes.

9.REFERENCES:

ISO/IEC 27005. (2018). *Information technology — Security techniques — Information security management.* ISO.

ISO/IEC 27001. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* ISO/IEC.