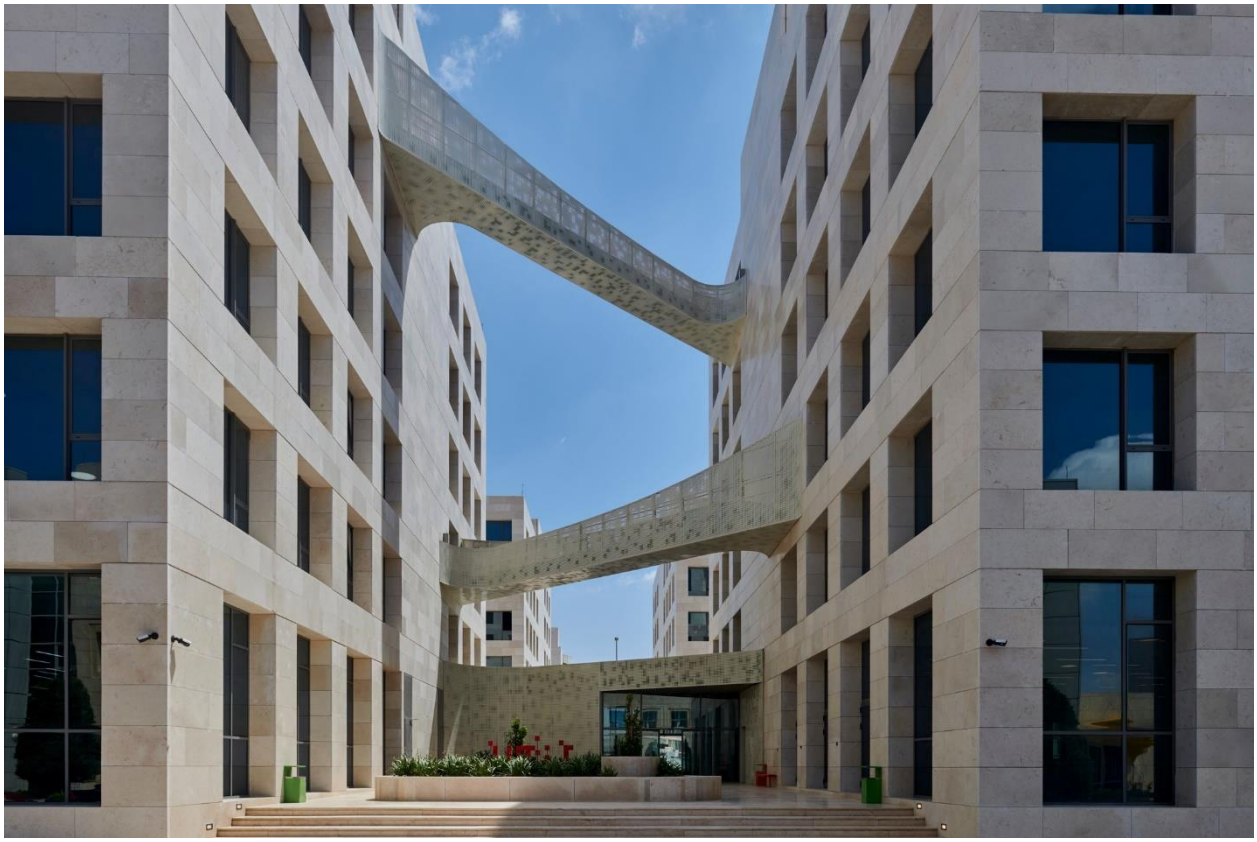
جامعة الحسين التقنية
Al Hussein Technical University



Student Name	Osama Mohammed Ziad Hasan
Student ID	23110709
HTU Course Number and Title	00203280 Security
Academic Year	2024-2025 Fall
Assignment Author	Hazem Arabiyat
Course Tutor	Rahmeh Ibrahim
Assignment Title	Future-Tec
Submission Date	25/1/2025

Table of Contents

Future-Tec scenario

Future Tec Company is a leader in banking security systems, offering innovative solutions and exceptional support. It ensures secure operations through advanced IT infrastructure, enhancing data management and compliance with financial regulations.

Key IT Servers & Systems:

- **Application Servers:** Manage banking inquiries, customer feedback, and support systems.
- **Database Servers:** Store client data, financial analytics, and interaction histories.
- **Web Servers:** Host the website and client dashboards for seamless access.
- **Communication Servers:** Handle emails and notifications for team-client interactions.
- **File Servers:** Organize storage and sharing of documents and materials.
- **Backup & Recovery Servers:** Ensure data integrity with regular backups and recovery.
- **Security Servers:** Protect against unauthorized access and cyber threats.
- **Monitoring Servers:** Oversee IT infrastructure health and performance.
- **Compliance Servers:** Maintain regulatory compliance and audit logs.

Customer Interaction Points:

- **Online Dashboard:** Monitors banking metrics and manages accounts.
- **Mobile Apps:** Enable banking security management on the go.
- **APIs:** Facilitate seamless service integration.
- **Payment Systems:** Secure online and contactless payment options.

Security Assessment & Key Findings:

1. **Endpoint Security Lapses:** Employees mix work and personal activities; devices lack updated anti-malware.
2. **Lack of Network Segregation:** No separation between critical servers, exposing sensitive data.
3. **Outdated Cryptography:** Reliance on MD5 raises security concerns.
4. **Backup Security Issues:** Unencrypted backups stored on public cloud services.
5. **Remote Administration Vulnerabilities:** Outdated OpenSSH versions need patching.
6. **Phishing & Physical Security Gaps:** Weak data center security and disaster recovery infrastructure.

7. **VPN Access Issues:** Unregulated access and expired digital certificates pose risks.
8. **Poor Password Management:** Employees write down passwords, leading to security lapses.
9. **Social Engineering Threats:** Employees fall victim to phishing attacks.
10. **DDoS Attacks:** External threats disrupt services and mask data breaches.
11. **Internal Threats:** Unauthorized access and data manipulation by employees.
12. **Physical Security Concerns:** Weak entrance security with outdated key systems.

As the Information Security Analyst, my report will highlight these vulnerabilities, assess their impacts, and propose strategic solutions to the CEO to strengthen security and reliability.

PART I

Risks of unauthorized use of systems

Unauthorized use of systems is the process of gaining access to a physical, electronic system without the permission of the administrator or owner. Such access can be obtained by bypassing security measures, exploiting system vulnerabilities or by using stolen credentials. It can happen internally, i.e. from an employee within the company, or externally.

Unauthorized use of systems may lead to many serious risks that vary according to the hacker's intent, such as:

1. **Theft of Money or Goods via Fraudulent Activity:** Hackers can carry out a variety of fraudulent activities when gaining access to sensitive data. These may include credit card fraud, manipulation of bank accounts, or even setting up fake businesses.
2. **Removal or copying of data or code:** Hackers may copy or remove sensitive data such as financial records, personal identification information, trade secrets, or intellectual property, or source code, for various purposes such as blackmailing the company, exposing the company's plans, or selling it to competing companies.
3. **Gain Physical control:** If the hacker gain control over an industrial control system, he can cause damage or destroy any equipment or machines.

These risks may cause consequences, such as:

1. **Economic damage**:
   - Loss of financial assets through theft or fraud
   - Cost of recovering systems.
2. **Reputational damage**:
   - Loss of trust from customers, stakeholders and the public.
   - Negative media coverage that affects the brand image and market value.
3. **Technological damage**:
   - Loss or exposure of proprietary technologies and trade secrets.
   - Increased likelihood of further attacks due to compromised systems.
4. **Physical damage**:

- Damage to industrial equipment or infrastructure caused by hackers with control over physical systems.
- Potential risks to employee safety arise as a result of system manipulation.

(Bakharev, 2024)

Security procedures

Defining security procedures:
Security procedures is the phase in which high-level policies are converted into specific, actionable steps and guidelines for implementing security measures. It provides a clear path and steps to implement, monitor and enforce security measures across the organization.

Examples for security procedures implemented by Future-Tec**:**

1. **Backup procedure:**

   The actions that must be taken in order to achieve the backup process:

   1. Identify systems, databases, and files to be included in the backup process.
   2. Categorize data and systems based on its sensitivity and retrieval priority.
   3. Perform monthly backups to be stored (Based on the company's policy).
   4. Encrypt all backups using advanced encryption standards to prevent any unauthorized access to them.

   Benefits of the backup procedure on the company:

   - Prevents data loss
   - Secure important information

2. **Recovery procedure:**

   When recovery process is needed, we must do these actions to recover backups as soon as possible:

   1. Find out what incident caused us to need the recovery.
   2. Assess the extent of data loss or corruption and identify damaged systems, and prioritize the recovery based on our categorization.
   3. Retrieve the most recent valid backup from the storage and restore critical systems and data based on the priority to reduce the downtime.
   4. Validate the integrity of the recovered data to confirm full functionality.

   Benefits of the recovery procedure on the company:

   - Reduce downtime by restoring systems as soon as possible
   - Recover lost, corrupted, or deleted data
   - Ensure business continuity

   (Most of the time Backup and Recovery are placed as one policy, but I decided to separate them in the procedure because the actions that are executed for each one of them are different.)

3. **Access Control Procedure:**

Actions needed to be taken ensure that only authorized personnel have access the company's critical systems:

1. Define access levels for employees based on their job roles and responsibilities.
2. Use multi-factor authentication for accessing the company's systems.
3. Monitor access logs continually to detect any attempt to get a unauthorized access.
4. Revoke access from an employee immediately when he leaves the company or when his role changes

Benefits of the access control procedure on the company:

- Prevent any unauthorized access to the company's systems, data, and physical spaces.
- Reduce the risk of data breaches, any threat or attacks.
- Enhances the company's security systems

The way each person applies a specific policy varies from one to another, but in the end the goal and purpose are the same, which is to benefit from it as much as possible and apply it in the best way that the cybersecurity expert sees fit in order to obtain a high-quality protection system. In my example, we benefited from each policy the best we can when it was implemented on the ground after it was just a policy, after focusing on assessing compliance with the procedures in place.

Method to assess and treat IT security risks

To assess IT security risks for Future-Tec, we have to identify, evaluate, and prioritize potential threats and vulnerabilities within the company. The implementation of each step:

1. **Risk identification:** It's the crucial step in the risk assessment process where we systematically identify and document every potential risk that could pose threats to the company's assets, operations, or objectives, that includes the following:

   - Asset identification: Here we identify assets to examine with the expertise of people in areas relevant to the company to identify key assets:
     1. Hardware Assets: Servers, networking devices, backup systems, employees' devices, storage devices and data centers.
     2. Software Assets: Operating systems, virtualization and cloud software, Security software, applications.
     3. Data Assets: Client databases, records
     4. Communication assets: Communication platforms and systems (e.g., Emailing, Messaging)

   - Threat Identification: Here where we systematically identify and document any potential threats that could exploit vulnerabilities and cause harm to the company's assets, operations, or objectives, that includes:
     1. Internal Threats: Insider attacks, accidental misuse of systems.
     2. External Threats: Hackers, phishing attacks, malware, DDoS attacks.
     3. Environmental Threats: Natural disasters.
     4. Operational Threats: Human errors, system misconfigurations.

- Vulnerability Identification: Here, we Identify exploitable flaws or weaknesses the company's IT systems or processes:
    1. Software Vulnerabilities: Lack of any of the company's system, access control malfunction due to misconfigured permissions
    2. Network Vulnerabilities: Lack of network segmentation, insecure configurations in firewalls, routers, or switches.
    3. Human Vulnerabilities: Poor password management practices leading to an unauthorized access, Lack of security awareness among employees.
    4. Physical Vulnerabilities: Access control malfunction in physical systems, Weaknesses in the company's IT infrastructure

- Analyze Existing Controls: To attempt to minimize threats that need to be identified, that includes:
    1. Management: Company's access and security policies
    2. Operational: Training employees on security awareness, periodic exercises to test incident response readiness.
    3. Technical processes and procedures: Firewalls and intrusion detection systems, encrypt sensitive data, backup and recovery systems for data integrity.

2. **Risk Analysis:** Now is the need to specify likelihood of occurrence of each identified threat to asset given existing controls, and specify consequence if the threat, whether qualitative or quantitative.

3. **Risk Evaluation:** In this Step, we compare the results of the risk analysis with the established risk criteria to determine where additional action is required. That can lead to a decision for each risk to one of:

    - Do nothing further
    - Consider risk treatment options
    - Undertake further analysis to better understand the risk
    - Maintain existing controls
    - Reconsider objectives.

4. **Risk Treatment:** In this step, we have to select and implement actions to address risks in a way that aligns with the company's goals, resources. Risk treatment options:
    - Risk Avoidance, which is to just avoid the risk completely and do not start or continue the activity that causes the risk. Use risk avoidance when the risk are too high and its potential negative impact is bigger than its benefits on the company.
    - Risk Acceptance, which is to take on or increase risks because the potential benefits outweigh the downsides, or because the cost of mitigation is higher than the impact of the risk. Use risk acceptance when the risk level is within acceptable range.

- Reduce Likelihood, which is to implement controls or measures to reduce the likelihood of risks occurring. Use reduce likelihood when we can manage the Risk through preventive measures.
- Reduce Consequences, which is to modify the structure or use of assets to reduce the impact if the risk materializes. Use reduce consequences when reducing the impact is more practical or more cost effective than reducing the likelihood of it occurring.
- Risk Transfer, which is sharing or transferring risk to another party, such as through contracts or insurance. Use risk transfer when the company wants to avoid standing the full impact of the risk.

Impact of misconfigured firewalls and VPNs

Security components in any organization, including tools, techniques, or processes designed to protect information technology systems, data, and networks from unauthorized access, misuse, or damage. To understand the reflection of the components on Future-Tec Company, we can see that these components work together to maintain the confidentiality, integrity, and availability of information and resources. Such as:

- Firewall, which provide a barrier between networks that prevents or denies unwanted or unauthorized traffic.

- Virtual Private Network (VPN), which is a technology that establishes a secure and encrypted connection over a public network.

However, in some cases misconfiguration of any of these techniques can occur in Future-Tec. Misconfigurations can arise from a range of sources, including weak passwords, improperly configured databases, unsecured cloud storage, misconfigured firewalls or network settings, and outdated software or firmware. It can lead to different types of cyberattacks, such as data theft, ransomware attacks, denial-of-service attacks, and malware infections. Cybercriminals exploit misconfigured systems and applications to gain unauthorized access, steal sensitive data, or disrupt business operations.

According to the 2022 Verizon Data Breach Investigations Report, misconfigurations were responsible for over 20% of all data breaches, we can understand from this report the extent of the danger of misconfigurations to the data of any organization, including Future-Tec.

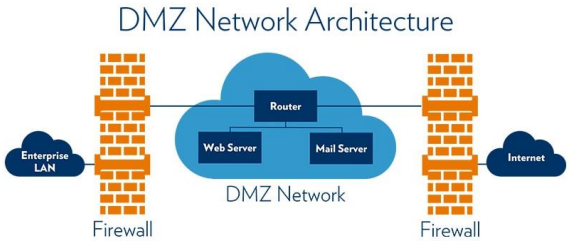
(Anon., 2023)

How Future-Tec Company can implement a DMZ

Demilitarized Zone (DMZ) is a designed network segment that provides the organization's internal network an additional layer of security by serving as a buffer zone between an organization’s internal network and external networks. That can lead us to host and expose public-facing services while isolating them from the internal network that contains sensitive resources and data.

We can implement DMZ on Future-Tec Company to enhance its network security, and reach a segregated public-facing services, By:

Putting two firewalls, one between the public internet and the DMZ network, to protect the DMZ from unauthorized or malicious traffic originating from the public internet by fencing off the DMZ network and prevent traffic to and from it, and the other between the DMZ and the enterprise LAN network internal network to protect the internal network from any threats in the DMZ network, in order to prevent anyone from gaining access inside the DMZ network.



Servers placed inside the DMZ:

- Web Servers: Publicly accessible content, such as websites or APIs, must be accessible by external users over the Internet.
- Mail Servers: External users can access email services without exposing the internal network to unnecessary risks by the web servers in the DMZ.
- Application Servers: To make it accessible to everyone without exposing any internal system.

Servers placed outside the DMZ:

- Database Servers: To ensure that sensitive and critical information are not directly exposed to any external threats.
- File Servers: To reduce the risk of unauthorized access or data breaches in the internal documents and data in the file servers.
- Backup and Recovery Servers: To isolate critical systems and data backups to not cause any attacks in the DMZ or external networks.
- Firewalls and Security Servers: To protect both internal systems and the DMZ itself.
- Monitoring and Management Servers: To ensure that attackers cannot easily to not messing around with security logs or take control of monitoring systems.
- Compliance and Audit Servers: To secure audit logs and data related to compliance, to maintain its integrity and confidentiality.

Benefits of Implementing a DMZ :

1. Enhancing Security:
   - Segregating public-facing services in the DMZ, to increase the level of security for the organization's internal network. This isolation helps protect critical systems and data from unauthorized access and potential attacks.
   - Using technologies such as firewalls to control the traffic into the DMZ and out of it would help protecting critical systems and data from unauthorized access and potential attacks.
2. Control Access:

- Allows organizations to carefully control the flow of traffic between the internal network and the external untrusted network
- It restrict and filter inbound and outbound connections with the services in the DMZ, ensuring that only necessary and authorized traffic is allowed.

3. Reducing Attack Surface:
   - Organizations can minimize the exposure of their internal network to potential threats by hosting public-facing services in the DMZ
   - The DMZ acts as a buffer zone, shielding the internal network from direct attacks or vulnerabilities that may arise from public-facing services.
   -

Network address translation (NAT) is a process used to translate private IP addresses that are used inside the company to public addresses that can be routed over the Internet.

Benefits of NAT for Future-Tec:

- Hides the internal IP addresses of devices within the company's network, reducing the risk of external attacks targeting specific devices.
- Future-Tec can have multiple internal devices that share fewer public IP addresses by using NAT, that helps save the costs associated with obtaining additional public IP addresses.
- Allows us to add more devices to their network without requiring public IP addresses for each device, to ensure that the network grows cost-effectively.

Static IP address is a fixed and unchangeable IP address assigned to a network or device, to remain constant, providing a reliable identifier for the device or service.

Benefits of static IP for Future-Tec:

- Access Control: Allows access only from specific IP addresses, organizations can create a whitelist of trusted sources, effectively blocking access attempts from unauthorized or suspicious IP addresses.
- Firewall Configuration: Enable Future-Tec to configure their firewalls more effectively, by setting it to allow or deny traffic based on specific IP addresses, effectively filter out potentially malicious traffic.
- Log Monitoring and Analysis: Static IP addresses simplifies log monitoring and analysis, to associate specific activities with known IP addresses, organizations can more easily identify and investigate security incidents, that helps the company to detect patterns, identify potential threats, and respond to security events in a timely manner.

Benefits of implementing network monitoring systems in Future-Tec Company

Implementing a network monitoring system is essential for any organization in order to ensure continuous monitoring of all systems, enabling us to detect and address any potential issues, anomalies, and security threats that may threaten its security.

Implementing network monitoring systems in Future-Tec Company will improve its overall infrastructure security, performance, and reliability by:

- Helping administrators and IT teams in the company to evaluate the performance of network devices, applications, and services by enabling monitoring of bandwidth utilization, packet loss, latency, and device availability.
- Detect any technical error in the network faster and more efficiently, by providing real-time alerts and notifications when detected, in addition to track network outages, device failures, or connectivity issues.
- Analyse network data on a historical and current level, which helps in predicting potential bottlenecks, and identify trends, peak usage periods, this helps the company when making any upcoming decisions regarding the network.
- Monitoring and identifying any suspicious activity on the network, in order to confront it early, by analyzing network logs and flow data.
- Facilitate compliance with regulatory requirements and industry best practices, by logging network activity and generating detailed compliance reports.

PART II

Evaluating physical and virtual security measures

There are many security measures that can be implemented by Future-Tec in order to ensure the integrity of the company's security. Security measures is categorized by physical and virtual measures. Some of security measures to be implemented by Future-Tec's:

Physical measures:

1. **Fire-Rated Doors:**

Fire-rated doors are designed to prevent the spread of a fire and smoke within a building. These doors are particularly important in data centers where fires could have dangerous consequences.

By using fire-rated doors, we contain fires into specific areas within a facility. It also provide critical time for evacuation and minimize damage to equipment and infrastructure.

Benefits of fire-rated doors:

- Prevents the spread of fire, safeguarding other areas.
- Allows safe evacuation of personnel and equipment.
- Limits damage to IT systems and critical infrastructure.

By implementing Fire-rated doors by Future-Tec, it will protect the companies' critical IT systems, ensuring minimal downtime and preventing catastrophic loss of data and hardware components. This measure ensures business continuity while meeting fire safety standards.

2. **Access Cards:**

Access cards are widely used in data centers to enhance security and control access to restricted areas, it grant access to specific places to employees or concerned officials

When using access cards, specific zones gain role-based access to, in addition, access cards can be deactivated immediately in case of loss or theft. We can integrate it with other security systems for enhanced monitoring.

Benefits of access cards:

- Simplifies access control without the need for physical keys.
- Cards can be quickly deactivated to prevent unauthorized access.
- Restricts access to authorized personnel only.
- Tracks and records all access events for compliance and incident investigations.

Future-Tec can use access cards to enforce strict access control in sensitive areas, such as server rooms and data centers. The audit trail and system integration features allow for effective monitoring, ensuring compliance and reducing insider threats. Lost or stolen cards can be deactivated immediately to maintain security.

3. **Biometric Devices:**

Biometric devices utilize unique physical or behavioral characteristics of individuals, in order to provide advanced security measures and enhanced access control in data centers.

Biometric devices can be used to serve as access control tools to restrict entry to only authorized individuals, can dispense with passwords or keycards, track employee attendance and prevent manipulation of records, integrate with other security systems for comprehensive protection.

Benefits of biometric devices:

- Ensures access is not given only to unauthorized users with verified biometric traits, which ensures the company's high-level security
- It eliminates password vulnerabilities, reducing the risks of password theft, sharing, or weak password usage.
- Links access events directly to individuals, enhancing transparency and security.
- Tracks time and attendance, to prevent attendance manipulation and ensures accurate workforce management.
- Works with surveillance and alarm systems for a comprehensive security ecosystem.

Future-Tec can benefit from biometric devices by authorizing specific users to ensure that no one else has access to sensitive areas, reducing the risk of insider threats and unauthorized entry. Audit trails and integration capabilities also enhance monitoring and incident response, enhancing overall IT security.

Virtual measures includes:

1. **Port Mirroring:**

A network monitoring method that allows a switch to make duplicate copies of traffic passing through a switch, and then sending it out a port with a network monitor attached.

The use of port mirroring enables network administrators to monitor and analyse network traffic patterns by duplicating traffic from a specific port or multiple ports, it helps detect anomalies or suspicious activities within the network by examining real-time traffic data, which identify any performance issues, such as packet loss or latency.

Benefits of port mirroring:

- It provide us detailed insights into network traffic without disrupting the original data flow.
- Helps identifying the cause of network issues quickly by analysing duplicated traffic.
- Ensures network activity is monitored and logged for compliance with regulatory requirements.

Future-Tec can implement port mirroring to gain deeper visibility into its network traffic to ensure real-time detection and resolution of performance issues or security threats. This method allows the IT team to proactively monitor network behaviour, identify potential anomalies, and maintain optimal network health. By integrating port mirroring with other network monitoring tools, Future-Tec can strengthen its security posture and ensure compliance with industry standards.

2. **Honeypots:**

Honeypots is a cybersecurity tools used to detect, deceive, and analyse attackers. They consist of intentionally vulnerable systems or networks designed to attract malicious actors, allowing security teams to study their tactics and gather intelligence.

Benefits of honeypots:

- Provides early warning systems by attracting attackers to non-critical systems, which enables organizations to detect and respond to threats before they escalate.
- Provides a controlled environment to study the behaviours of the attackers, and their tools, and techniques.
- Divert attackers away from production systems, which reduce the risk of compromising critical data or infrastructure.

Implementing and setting honeypots within Future-Tec's network can make the unauthorized access attempts detection easier for us, and improves the defences against evolving potential attack methods. Diverting attackers to honeypots can reduce the risks to the company's production environment, ensuring business continuity.

3. **Virtual Private Network (VPN):**

A technology that establishes a secure and encrypted connection over a public network, such as the internet, creating a private network that securely extends across the public infrastructure.

Benefits of VPN:

- Enhances security using encryption to protect sensitive data, such as passwords, financial details, and personal information, from interception and any unauthorized access.
- Masks IP address and encrypt internet traffic, which make it difficult for anyone to track your online activities.
- Enables access to content, websites, or services that might be blocked in our region, ensuring unrestricted browsing, by allowing us to bypass geographic restrictions or censorship by connecting to servers in different locations.

Implementing VPN in Future-Tec can enable employees to access company resources securely from remote locations. It also ensures all data exchanges between remote devices and central servers are encrypted, safeguarding sensitive client and business information.

Qualitative risk analysis

Future-Tec is exposed to many risks, some of which can affect hardware, software, and data assets, potentially putting its reputation at risk. If left unaddressed, these risks could disrupt critical systems, compromise sensitive information. To better understand and mitigate these challenges, risks can be divided into three main types of assets, which is hardware, software and data Assets

Asset	Threat/ vulnerability	Existing controls	impact	Likelihood	Level of risk	Suggested control
Corporate network/ Software asset	No segregation between critical servers	Basic firewalls	unauthorized access to critical servers, leading to loss on many levels.	Likely	High	Implement VLANs to isolate servers and monitor network traffic.
Remote access systems/ Software asset	OpenSSH versions in the organization are outdated and need immediate patching and access control improvements.	Old OpenSSH versions	May lead to Unauthorized access, data breaches	Possible	Medium	Upgrade OpenSSH versions, apply restrict access
Employee endpoint devices/ Hardware asset	Employees use their devices for both work and personal purposes	No control	Increasing the risk of malware introduction, which may cause data loss, spread malware	Likely	Medium	Set strict rules and limits on what can be accessed on work devices, whether via the Internet or downloadable applications.

			across the systems			
Physical Security/ Hardware Asset	Use of glass doors for main entrances without adequate reinforcement and outdated physical key systems	Basic key lock system	Unauthorized physical access, theft of equipment.	Possible	Low	Implement smart locks with access control cards for glass doors
User authentication system/ Software and hardware asset	Employees' poor password management, including physically writing down passwords	No access	Unauthorized access to the company's systems, including servers, databases, and networks	Likely	High	Set rules for building a strong password, apply MFA (Multi Factor Authentication) policy
VPN System/ Software asset	VPN Access Issues	Unregulated VPN access and expired certificates	Unauthorized access to internal systems, potential data breaches, loss of reputation with clients	Possible	High	Set strict VPN policies, renew certificates regularly
Web Applications/ Software Asset	External attacks disrupt services and mask potential sensitive data breach attempts.	Limited DDoS protection	leads to financial and reputational loss, and unauthorized data access.	Likely	High	Use DDoS mitigation tools
Customer Data Backup/ Data Asset	Backup stored on a public cloud service without encryption at rest.	Regular backups	Unauthorized access and exposure of sensitive customer data	Likely	High	Encrypt backups at rest and in transit
Data Center/ hardware asset	Lack of UPS in the data center.	Lack of physical security	Unauthorized physical access	Likely	High	Install a UPS system

I chose these assets to be diversified in terms of type and level of risk, and some of them were very important to me, so I gave them priority over other assets.

Data protection regulations applicable and procedures implemented

Security regulations are local global rules and guidelines that organizations must follow in order to protect their data and technology infrastructures. We can categorise security regulations into local, global regulations.

Future-Tec, as a company in the banking security industry, must comply with strict data protection regulations to secure client's information, maintain trust, and not violate any legal laws. The two primary regulations applicable are:

1. **General Data Protection Regulation (GDPR):**

   A detailed rules about data privacy and protection that applies to organizations handling personal data of people within the European Union (EU). Procedures Future-Tec implements to comply with the GDPR regulation:

   - Process the personal data of clients, including financial analytics, interaction histories, and clients' profiles.
   - Provide specific training to employees to ensure they understand their responsibilities in protecting personal data.
   - Publish honest privacy policies to inform clients about how their data is being collected, processed, and secured, to reassure them and gain their trust, increase organization's reputation and not getting into any legal problems.

2. **Payment Card Industry Data Security Standard (PCI-DSS):**

   A set of security standards developed by the major payment card brands like (Visa, Mastercard, American Express, Discover, and JCB) to protect the cardholder's data. Procedures Future-Tec implements to comply with the PCI-DSS regulation:

   - Handle sensitive payment card information, like card numbers, cardholder names, and expiration date using the most powerful means of protection, to ensure that this data is securely processed.
   - Set protocols for notifying payment card brands and affected clients as soon as possible in case of a breach, In order to reduce the damage as much as possible.
   - Make monthly plans for training employees on PCI-DSS compliance, focusing on secure handling of cardholder data.

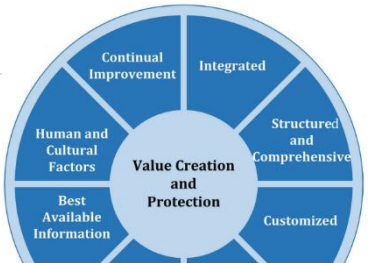
ISO 31000 risk management methodology and its application

ISO 31000 risk management purpose is to create and protect the value within an organization. It improves the performance, encourages innovation and supports the achievement of objectives by offering a structured approach to managing risks.

(I summarized the methodology and its implementation on Future-Tec in the same context)

The risk assessment methodology is guided by the principles of ISO 31000, which is the foundation Future-Tec to manage risk and should be considered when establishing Future-Tec's risk management framework and processes. For these principles to apply to our risk assessment methodology, the following must be met:

1. Integrated



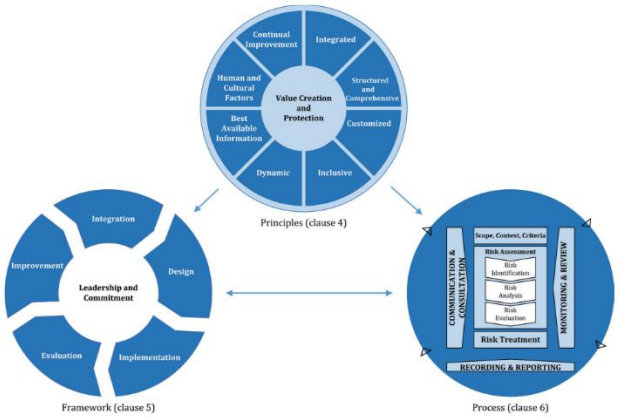
2. Structured and comprehensive
3. Customized
4. Inclusive
5. Dynamic
6. Best available information
7. Human and cultural factors
8. Continual improvement

After ensuring that all principles are applied, the framework comes into play, which assists the company in integrating risk management into significant activities and functions. Within the framework, the organization should evaluate its risk management's practices and processes, and any gaps with its address. The way in which framework components work together should be customized to the needs of the organization.
Leadership and commitment ensures the customizing and implementing of the framework on the level of all components, It include:

1. Integration: Understand Future-Tec's structure, goals.
2. Design: Customize the risk management framework to address challenges facing us and give clear roles and responsibilities for risk management.
3. Implementation: Establish risk management processes across all company's departments, and provide training and tools.
4. Evaluation: Assess the effectiveness of our risk management processes, Identify gaps and address.
5. Improvement: Create an analytic reports where lessons learned from incidents.

Process is one of the most important key characteristics, which involves the systematic application of policies, procedures and practices to the activities of communicating and consulting in Future-Tec, establishing the context and reporting risk after going through all the stages of studying it. The stages that must be passed through to complete the processing:

1. Communication and consultation to help stakeholders in the company understand risks, how decisions are made, and why certain actions are needed.
2. Establish the scope, the context and criteria to customize the risk management procedure in order to facilitate an efficient risk assessment and suitable risk management.
3. Risk assessment, including three main characteristics:
   - Risk identification, find, recognize and describe risks that might help or prevent an organization achieving its objectives.
   - Risk analysis, to understand the nature of the risk, such as where appropriate, the level of risk.
   - Risk evaluation, to support decisions.
4. Risk treatment, select and implement options for addressing risk.
5. Monitoring and review, to insure and improve the efficacy and quality of the process design, execution, and results.
6. Recording and reporting, to improve risk management activities.



We can apply ISO 31000 in Future-Tec in many forms, such as:

1. IT Infrastructure Security: To identify vulnerabilities in servers, networks and firewalls that could expose Future-Tec to cyberattacks, ransomware or data breaches.
2. Web Application Security: To identify risks related to the web applications, such as DDoS attacks, SQL injection, or unauthorized access to data.
3. Physical Security: To identify gaps in physical security, such as unregulated access to server rooms or weak locks on doors.
4. Disaster Recovery: To identify risks to business continuity, such as power outages, server failure, or natural disasters.
5. Customer Data Protection: To identify risks such as malware introduction or data leak caused by employees misusing devices.

IT security audits and their impact on the company

Security audits is the processes of examining and evaluating the security measures and controls within an organization's IT infrastructure. Its purpose is to identify vulnerabilities, assess potential risks, and verify compliance with security policies, standards, and regulations, it involve reviewing various components of an organization's IT systems, networks, applications, and data to evaluate the effectiveness of existing security measures and uncover potential vulnerabilities.

Security audits helps us as Future-Tec to identify the vulnerabilities by enabling us to uncover weaknesses in its IT infrastructure, including outdated software, misconfigured systems, and unpatched vulnerabilities, which can reduce the organizations' exposure to threats such as data breaches, ransomware attacks, and insider threats. It also can provide us a clear understanding of the risks related to different aspects of the organization's IT systems, networks, and applications, in addition, security audits ensure the compatibility between Future-Tec and industry standards and regulations, such as GDPR and PCI-DSS.

PART III

How IT security can be aligned with organizational policy

Organizational policies are the guidelines and rules that set the principles for the company and how it operates in its entirety, from defining the company's values and goals to everything related to the behaviour of everyone in the organization and daily decisions.

Some policies complement each other by aligning their objectives and working together to create a cohesive framework, for example:

Access Control Policy: Only authorized personnel are allowed to access sensitive data and systems.
Data Protection Policy: All sensitive data must be secured from unauthorized access using encryption.

This example shows us the compatibility between a global IT security standard for access control and a company-specific organizational standard that ensures the achievement of that global one, making it clear and without any loopholes to cross.

However, sometimes misalignment occurs, for example:

Clients Rights Protection Policy: It is strictly prohibited to use clients data for any purpose without their permission.
Clients Data Usage Policy: Employees have the right to use customer data for research purposes.

These conflicting policies create a loophole, allowing violations to occur and potentially compromising the organization's integrity and compliance.

Security impact of misalignments:

- Loopholes in policies, such as unclear data usage permissions, can lead to insider threats.
- Can confuse employees, leading to poor implementation of security measures.
- Inconsistent policies on data usage or access control can lead to unauthorized access
- Conflicting policies can lead to increasing in vulnerabilities, such as create gaps that attackers can exploit

Roles of stakeholders in implementing audit recommendations

Stakeholders plays important role in security auditing by ensuring the process is effectively implemented and aligned with the organization's goals. Their collective efforts focus on addressing risks, applying recommendations, and improving overall security to protect the organization's assets and ensure compliance with policies and regulations.

To make the roles of stakeholders clearer, here is a practical application of it on Future-Tec detailing all the roles:

1. **Manager:** Mr. Osama Hasan

   The manager ensures that security audit recommendations are implemented in a timely and effective manner. In the case of Future-Tec, Osama audits and supervises the resources and assesses whether they are sufficient or not, and monitors the overall progress of local and international standards at all levels and ensures that they are Keeping up with the company to date.

2. **IT Officers:**

An IT officer implements the technical security measures recommended by the security audit and ensures that these measures do not negatively impact the performance of the system. IT Officers application on Future-Tec:

IT Officer	Job Title	Role
Mr. Wessam Al-Shatarat	Network Security Expert	Manages network security, configures firewalls, and monitors for unauthorized access.
Mr. Mohammed Sammour	Data Protection Officer	Supervises data protection, ensures encryption protocols are in place, and manages backups.
Mr. Hatem Al-Shwayat	System Administrator	Ensures all systems are updated, manages patch deployments, and ensures system stability.

3. **Risk Owner:** Mr. Zaid Kamal

   Zaid makes sure that the company reduces the risks related to the security flaws found by the security audit. To put the suggested measures into action and ensure that the risks are manageable, Zaid must collaborate with management and IT, to create a detailed risk reduction plan based on the findings of the security audit, and use risk assessment tools to continuously monitor and re-evaluate risks after the reduction.

4. **Facility and security specialist:** Mr. Mahmoud Ammar

   Mahmoud makes sure that the company's data center and buildings are physically secure. He must ensure that the data center is secure and that the suggested security measures are implemented. In the company, the enhancement of physical security by installing access control systems like biometrics and access cards at the data center tasks is given to Mahmoud.

5. **Risk and Compliance:** Mr. Abdulrahman Hakam

   Abdulrahman's role is to make sure the company complies with the security audit's recommendations. To guarantee that the suggested actions are carried out and that the organization complies, Abdulrahman collaborates with other stakeholders to ensure audit recommendations are implemented and documented, he regularly review compliance with security regulations, such as GDPR, PCI-DSS and address any gaps.

Designing and implementing security policies

Policies are a set of high-level rules, guidelines, and directives that ensure the security of a company's systems on all levels. There are 3 types of security Policies:

Enterprise Information Security Policy (EISP):

EISP is a high-level policy that defines the outlines of the organization's general information security strategy. Detailed example of EISP on Future-Tec:

Password Policy:

Importance:
A strong password is crucial to have in the company, for safeguarding systems and sensitive data. It helps preventing unauthorized access, any internal or external threats.

Scope:
All employees, workers, and systems in the company

Policy:

- Any password in the company should have more than 9 characters
- Passwords should be changed every 100 days

Tools:

- Microsoft PowerShell for checking password validation and expiry, to check whether passwords meet complexity, length, and expiration requirements by querying system policies. I choose Microsoft PowerShell because it's built into Windows environments, making it the ideal for the company.
- Hashcat for encryption, Ensures passwords are hashed using secure algorithms. I choose Hashcat because it's widely strong and trusted tool for testing and verifying the strength of password encryption

(Anon., 2011)

Issue-Specific Security Policy (ISSP):

ISSP focuses on a specific issue itself or areas that need to detail its guidelines. For example, how to handle email, internet use, or data privacy. Detailed example of ISSP on Future-Tec:

Backup and Recovery policy:

Importance:
Backup and recovery servers are important for ensuring data integrity and minimizing disruptions. Regular data backups and swift recovery protocols in case of data loss are critical to maintaining business continuity and securing sensitive information.

Scope:
All critical systems and data repositories within the organization.

Policy:

- The company must perform monthly schedule backups for all critical systems and databases.
- Backups must be stored in multiple locations, including on-site servers and cloud storage.
- Recovery protocols must be tested regularly, and any issue identified during testing should be addressed to improve recovery times.

Tools:

- Acronis True Image for backup Software, to automate the process of creating backups, ensuring data is consistently saved according to the organization's

schedule. I chose Acronis True Image because it has to many features that will make out backup strong, like disk cloning, cyber protection and strong privacy tools, which makes it my choice over other options like Commvault and Rubrik.
- Microsoft OneDrive for cloud storage, to provide a secure and scalable location for off-site backups, offering protection against on-premises failures. I chose OneDrive because we need security, performance, and a system that can work seamlessly with other systems together in one domain across all phases, which microsoft gives in its services. Microsoft OneDrive also ensures redundancy and quick accessibility during recovery efforts.
- Acronis True Image is also my choose for testing, to facilitate simulations to test backup integrity and the effectiveness of recovery processes. I chose Acronis True Image because it's the software I save my backup in, so it's easier to test.

(Anon., 2015)

System-Specific Security Policy (SSSP):

SSSP focuses on a specific systems, provides detailed rules for it, for example, how a services should be secured. Detailed example of SSSP on Future-Tec:

Servers monitoring and management policy:

Importance:
Monitoring and management servers play a big role in monitoring the health and performance of the IT infrastructure in the company. They enable potential issues to be identified and resolved proactively, ensuring smooth and uninterrupted operations.

Scope:
All critical servers to IT infrastructure, including FTB, database, and other servers.

Policy:

- Continuous monitoring must be implemented to track system health, performance, and security in real-time
- Implement weekly performance reviews to identify trends, bottlenecks, and areas for enhance.
- putting plans to upgrades and resource allocation effectively by monthly analysis.

Tools:

- Datadog for the monitoring possess, I chose Datadog because it's a many in one monitoring tool, it can monitor servers, applications, databases, cloud infrastructure, and networks, and in addition, it integrates with over 500 tools and services with customizable dashboards.
- Splunk from cisco for the log management and analysis, I choose Splunk because it can aggregate logs from multiple servers for centralized visibility, and enables real-time search, visualization, and analysis of server events.
- Ansible for the automation and configuration, I choose Ansible because it's agentless and simple, but at the same time, it is a powerful performer for automation, it automates repetitive tasks like server configuration and updates, and scales easily across large server infrastructures.

- Nagios for security monitoring, to proactive infrastructure monitoring. I chose Nagios because it's performance in monitoring server performance, services, and network traffic for issues is so strong, and detects security vulnerabilities in real-time.

(Anon., 2025) (Anon., 2025) (Anon., 2023) (Anon., 2025)

Disaster Recovery Plan (DRP) is an entails preparation for any disaster and recovery from it if happened, whether natural or human made. to implement DRP on Future-Tec, here is our components:

Step 1. Plan For Disaster Recovery:

We have to generate these documents:

1. List of covered disasters under Future-Tec
   - Natural Disasters: Tornadoes, Earthquakes, Hurricanes, Hurricanes
   - Human Made: Cyberattacks, Physical damage to the company's systems or infrastructure, Power outages
2. List of disaster recovery team members for each type of situation and their contact information

IT Officer	Role	Contact Information
Mr. Saad aqqad	DR Manager	Phone: +962-780089884, Email: Saad.aqq @ ft.jo
Mr. Omar Jabalawy	Backup Expert	Phone: +962-791275949, Email: omar.jab@ ft.jo
Mr. Mohammed Eyad	IT Infrastructure Specialist	Phone: +962-778538739, Email: moh.eyad@ ft.jo

3. Backup documentation
   We need to document every backup we have done previously for the company
4. Restore documentation
   We have to document every restoration we have done previously for the company

Step 2. Crisis Management:

We have to involve the following:

1. Strategies
   - Address potential threats such as cyberattacks, natural disasters, or system failures.
   - Create scenario-specific plans tailored to many identified risks.
2. Processes
   - Monitor systems and operations to detect and confirm crisis situations promptly.
   - Assess the extent of the crisis to determine response efforts.
3. Actions

- Inform employees, stakeholders, and clients about the plans and every regular update.

We use these steps to manage a crisis situation effectively and reduce its effects on people, organizations, and communities.

Step 3. Recovery Operations:

The actions taken to restore normal operations and rebuild after a crisis or disaster, such as:

- Limit the impact by isolating affected areas, whether physical or digital
- Implement our recovery plans, such as restoring systems from backups or redirecting operations to alternative facilities.
- Offer financial and emotional support to affected individuals and their families, whether they are employees and clients.

However, these recovery operations may vary, depending on the nature of the disaster and the impact it has had on the affected area or organization.

Critical assets of the company, developing a security plan

Critical assets to develop a comprehensive security plan to safeguard them:

1. **User Authentication System:**

   Why do we need to safeguard the User Authentication System: There is poor password management in the company's services at both levels:

   - Software level, Weak written down physically passwords for all systems, and no multi-factor authentication (MFA).
   - Hardware level, Weak IT infrastructure passwords, and unsecured login mechanisms.

   Impact of leave it without safeguarding: These problems may lead to unauthorized access or possible theft within the company's buildings or within its systems, which can cause a reputational, financial, technical damage and compliance Issues.

   The controls we currently have:

   - Basic password and control access policies
   - Weak physical locks

   Actions to stop the risks:

   Enforce Strong Password Policies:

   Strong password policies are critical for securing user accounts, systems, and sensitive data in the company. We can implement that by requiring passwords to:
   - Any password in the company should have more than 9 characters
   - Passwords should be changed every 100 days

   Applying Multi-Factor Authentication (MFA):

   MFA adds an extra layer of security by requiring users to provide two or more authentication factors. We can implement that by requiring the following:

- Password
- Biometric authentication

2. **Physical Security:**

Why do we need to safeguard the physical Systems: Future-Tec glass doors for main entrances that do not have sufficient and outdated physical key systems, these reasons can lead to clear security risks.

Impact of leave it without safeguarding: Failure to pay attention to physical security in the company may lead to serious consequences, such as unauthorized physical access, and theft of physical assets due to the weakness of this asset in the company building.

The controls we currently have:

- Weak glass doors for main entrances
- Outdated physical key systems

Actions to stop the risks:

Strengthening the glass used in the doors:

A strong glass doors make the challenge difficult for hackers to cross from an entry points, thus preventing unauthorized physical access. We can implement that by:
- Replace weak glass doors with reinforced security glass
- Add metal frames or secure glass panels

Upgrade to Smart Locks:

Smart locks record every access attempt, provide us a log of who accessed a specific area and when. We can implement that by requiring:
- An access card to enter any of the company's doors.
- Install CCTV cameras with motion detection at entry points and critical areas inside the company.

3. **VPN System:**

Why do we need to safeguard VPN System: Future-Tec faces annoying issues in this regard, as there is lack of control over who can connect to the VPN, and the company's digital certificates for VPN are expired.

Impact of leave it without safeguarding: These issues makes it possible for unregulated VPN access to be exploited to enter to these systems by malicious users, in addition to exposing sensitive company or customer data.

The controls we currently have:

- Unregulated access to VPN
- Expired certificates for VPN

Actions to stop the risks:

Set Strict VPN Policy:

Without policies, anyone with VPN credentials can access the system without restrictions, that can increase the risks. This policy state that:

- Only limited IP addresses or geolocations are allowed or for VPN connections.
- Allows VPN configuration to connect only during business hours.

Renew and Automate Certificate Management:

Attackers may exploit the certificates expire to intercept VPN traffic or impersonate the organization, resulting in unauthorized access. We can implement this by

- Renew all expired certificates immediately and replace them.
- Use automated certificate management tools to prevent this problem from happening again.

I have selected these particular assets based on security priority in order to develop a security plan for them. All of the problems I have mentioned are serious and may lead to more problems than others.

References

BrightSec. (2024) Unauthorized Access: Risks, Examples, and 6 Defensive Measures. Available at: https://brightsec.com/blog/unauthorized-access-risks-examples-and-6-defensive-measures/#:~:text=When%20unauthorized%20individuals%20gain%20access,reputation%2C%20and%20potential%20legal%20repercussions.

Kiteworks, (2023). Security Misconfiguration Vulnerabilities: Risks, Impacts, and Prevention. Available at: https://www.kiteworks.com/risk-compliance-glossary/security-misconfigurations/

Acronis, (2015). Acronis Cyber Protect Home Office (formerly Acronis True Image). Available at: https://www.acronis.com/en-us/products/true-image/

Datadog, (2025). Datadog: Cloud Monitoring as a Service. Available at: https://www.datadoghq.com/

Splunk, (2023). Log Management: What is it and why it matters. Available at: https://www.splunk.com/en_us/blog/learn/log-management.html

NetApp, (2025). What is Ansible Configuration Management?. Available at: https://www.netapp.com/hybrid-cloud/it-automation/what-is-ansible-configuration-management/

Hashcat. (2011). Hashcat Wiki. Available at: https://hashcat.net/wiki/