A picture containing logo

Description automatically generated

**Security**

**10203280**

**(D/618/7406)**

**Section (9)**

**Submitted To:**

Dr. Safaa Hriez

**Submitted By:**

Farouq Hassan

Fall 2022

**Table Of Contents**

* 1. Part A ……………………………………………. (3)

2.1. Part B …………………….………………………… (8)

3.1. Part C …………………………….…………………….……… (14)

4.0. Part D …………………….…………………………………… (16)

4.1. A …………………….…………………….………………………… (16)

4.2. B…………………….………………………………………………… (16)

4.3. C…………………………………………….………………………… (17)

5.1. Part E…………………….………………………… (19)

6.1. Part F…………………………………………………. (21)

7.1. Part G………………………………….…………….……... (24)

8.1. Part H, I,J ………………………….……………….…... (25)

9.1. Part K………………………………………………….…... (32)

10.1. Resources………………………….……………….…... (34)

**------------------------------------------------------------------------------**

**Part A**

Discuss the most critical assets of the Warmaksan's system, considering their CIA principles in mind.

|  |  |  |
| --- | --- | --- |
| Asset name | Why is it valuable? | CIA principles affected  Confidentiality, integrity, availability |
| Hardware (endpoints / servers / storage devices / cables / networking devices / cloud infrastructure / Monitoring stations / Data center) | 1- The endpoints (PCs / Laptops / mobile devices / tablets):  allow the company to communication with each other and clients, and customers via messages or emails and keep updated with everything in the company or any issues faces the customers to fix it through all the way above  2- Servers and storage devices:  allow warmaksan to store and process data and that contain all the customer and employees and the application information and the operation system for the warmksan and let the devices like the PCs access and share resources, and applications  3- cloud infrastructure:  allows warmksan to access computing resources, and storage on demand, and without having to invest in and maintain on their own hardware. This could provide scalability and flexibility, as resources can be easily increased or decreased as needed.  4- cables networking devices:  they are necessary for connecting devices and Facilitate communication and the data and information transfer between the devices in the company and give the internet to every single device  5- Data center:  This is a physical location where networking devices and servers are stored and where data is processed and stored.  For all the above:  These devices allow the employees to process and access the information, collaborate, and communicate with each other’s, and access resources and applications that are necessary for their work. | Confidentiality: Hardware assets that contain sensitive information, such as confidential data, financial records, and customer information, are vulnerable to unauthorized access or theft. To protect the confidentiality, hardware assets should be secured with proper access controls, such as passwords, biometric authentication, and encryption.  Integrity: Hardware assets that are used to store, process, or transmit data must be protected from unauthorized modification, deletion, or tampering. To ensure integrity, hardware assets should be regularly backed up, physically secured, and monitored for suspicious activity.  Availability: Hardware assets must be available and functioning when they are needed. Interruptions to availability, such as hardware failures, network outages, and cyber-attacks, can have a significant impact on the operations of Warmaksan. To ensure availability, hardware assets should be regularly maintained, updated, and protected against threats.  The confidentiality of data on or transmitted can be affected and the availability of endpoints can be impacted.  The confidentiality and integrity of data transmitted over cables can be affected.  The confidentiality, integrity, and availability of data stored on storage devices and servers, services that are hosted in the cloud, monitoring stations, and data centers, and data transmitted through networking devices, can be affected. |
| Software (Application Operating system, Security software, Backup and recovery software) | 1. Operating system:   It is an important software asset, as it is responsible for managing and controlling system hardware resources. Ensuring from the integrity, and availability of the operating system is something essential to maintaining system performance and reliability.   1. Application:   This that Warmaksan offers it can be a critical software asset, because they are the primary means by which customers interact with the system, communicate in messages or videos, and get to each other by it, and how handle with the system.   1. Security software:   It is such as an antivirus, firewall or other applications that are important to the security of the Warmaksan system. Ensuring proper operation and configuration of these asset is essential to maintaining system security.   1. Backup and recovery software (cloud software):   it is an important thing to the availability of Warmaksan's system, because it ensures that is the system can recover from disasters, or failures. | Confidentiality: Confidentiality ensures that sensitive information is protected from unauthorized access or disclosure. Software assets in Warmaksan could be affected by confidentiality breaches if they are not protected by secure login credentials, encryption, and other security measures. Confidential information stored on software assets could be vulnerable to theft or unauthorized access if adequate protection measures are not in place.  Integrity: Integrity ensures that information is accurate, complete, and protected from unauthorized modification. Software assets in Warmaksan could be affected by integrity breaches if they are not protected by firewalls, intrusion detection systems, and other security measures. Attackers could modify or manipulate software assets to compromise the accuracy and completeness of the information they contain.  Availability: Availability ensures that information is accessible and usable when it is needed. Software assets in Warmaksan could be affected by availability breaches if they are not protected by disaster recovery plans, backup systems, and other measures that ensure the availability of data. Attackers could cause software assets to be unavailable through denial of service (DoS) attacks, data corruption, and other means.  The confidentiality, integrity, and availability of data processed by application software, operating system, security software, and backup and recovery software, of them can be affected by threats, improper access controls, and security vulnerabilities. |
| Data (data on Disks, Customer information) | Customer information:  It has all the information financial or personal for the customers and stored in warmaksan. And that could include information such as logs, addresses, payment details, emails, passwords, phone number and names.  data on Disks:  It helps to store the data in warmaksan, which refers to the data stored on the physical disks and that's such as solid-state or hard drivers, and that could include the files, applications, documents | Confidentiality: Confidential data should only be accessible by authorized individuals. The unauthorized access or disclosure of confidential data can result in significant harm to Warmaksan. This can be achieved through the use of strong access controls, encryption, and secure data storage solutions.  Integrity: Data integrity means that the data is complete, accurate, and consistent. A breach of data integrity can occur if unauthorized changes are made to the data or if data is accidentally or maliciously altered. This can result in incorrect decisions being made based on the data or a loss of trust in the data. To ensure data integrity, Warmaksan can implement data validation, backup, and disaster recovery procedures.  Availability: Data availability refers to the ability of authorized individuals to access the data when they need it. A loss of data availability can occur if the data is unavailable due to a system failure, network failure, or a security breach. To ensure data availability, Warmaksan can implement redundancy, disaster recovery, and business continuity plans.  The confidentiality, integrity, and availability of data stored on disks (SSD/HDD), and customer information, of them can be affected by threats, improper access controls, and security vulnerabilities. |
| Networking (Subnet / Internet connection / web application / VPN) | Subnets:  Allow the network to divided into a smaller, based on a physical or logical criteria, like function or location. and could be more manageable, and it can help prevent unauthorized access to the warmaksan network by limiting the access into specific segments.  Internet connection:  Allow warmaksan to connect to other network and share or transfer the information and data into the internet, and access many of services and recourses like the cloud or web or emails or communicate with the customers via social media or web site or application, and help to connect with the whole world.  web application:  it helps to provide the services and recourse in a very comfortable way to engage with the employees and the customers, like customer portals, and online profile…ect.  Virtual private network (VPN):  Allow remote users for employees and customers or even partners into the corporate network, and to protect sensitive data by encrypted to be secured from unauthorized access | Confidentiality: Unauthorized access to sensitive information that is transmitted over the network, such as confidential client information, internal communication, and financial data can compromise the confidentiality of the data.  Insufficient encryption protocols or weak passwords can make it easier for attackers to penetrate the network and access confidential information.  Integrity: Attackers can launch a man-in-the-middle (MITM) attack to intercept and manipulate data in transit. This can lead to data being altered, corrupted, or destroyed, compromising the integrity of the data, Malware, and viruses can infect the network and cause harm to the systems and data, leading to a loss of integrity.  Availability: Distributed denial-of-service (DDoS) attacks can cause the network to become unavailable, leading to loss of business operations and revenue, and Unauthorized access to the network or devices within it can cause the network to shut down, resulting in downtime and loss of availability.  The confidentiality, integrity, and availability of data transmitted within a subnet, web application, VPN, and Internet connection can be affected by threats, improper access controls, and security vulnerabilities.  In addition, the VPN network and the Internet connection itself can malfunction due to technical malfunctions or other disturbances. |

**Part B**

Discuss and assess Warmaksan system's possible risks, their likelihood (rare, unlikely, possible, likely, and almost certain), and exploitation consequences (insignificant, minor, moderate, major, catastrophic, and doomsday).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Asset name | Threat/  Vulnerability | Existing  control | Likelihood | Consequence | Level of risk | Risk priority |
| endpoints | Malware, phishing attacks, and physical theft or loss, unsecured wireless networks / weak passwords, and a lack of security software, and outdated software. | not all existing devices within the offices are well secured | Possible | Major | High | 6 |
| Servers | malware, physical damage or malfunction or theft, and unauthorized access hacking / unpatched software, weak passwords, misconfigured security settings. | are easily accessed by anyone. | Almost  certain | Major | Extreme | 4 |
| Storage devices | malware, physical damage or malfunction or theft, and unauthorized access / weak passwords, misconfigured security settings, a lack of encryption. | are easily accessed by anyone. | Almost  certain | Major | Extreme | 5 |
| cables | unauthorized access or tampering, physical damage / a lack of insecure connections or physical security measures. | are easily accessed by anyone. | likely | Minor | High | 10 |
| Networking devices | malware, and unauthorized access, hacking, physical damage or theft / unpatched software, weak passwords, and misconfigured security settings. | there are misconfigurations on network security devices such as firewalls and VPNs | Possible | Minor | Medium | 14 |
| Cloud infrastructure | malware, and unauthorized access, hacking / unpatched software, weak passwords, and misconfigured security settings. | ---- | Possible | Minor | Medium | 12 |
| Monitoring stations | malware, and unauthorized access, hacking / unpatched software, weak passwords, and misconfigured security settings. | It is not mentioned | Possible | Minor | Medium | 13 |
| Data center | malware, and unauthorized access, hacking, physical damage or theft / unpatched software, weak passwords, and misconfigured security settings. | the data center's door can be easily opened, and the servers and networking devices are easily accessed by anyone | Possible | Doomsday | Extreme | 1 |
| Applications | malware, unauthorized access, and weak passwords / weak passwords, unpatched software, and misconfigur ed security settings. | It is not mentioned whether any controls are in place to secure | Possible | Minor | Medium | 11 |
| Operating system | malware, unauthorized access, and weak passwords / weak passwords, unpatched software, and misconfigured security settings. | It is not mentioned whether any controls are in place to secure | Possible | Moderate | High | 7 |
| Security software | malware, unauthorized access, and weak passwords / weak passwords, unpatched software, and misconfigured security settings. | It is not mentioned whether any controls are in place to secure | Possible | Moderate | High | 8 |
| Backup and recovery software | malware, unauthorized access, and weak passwords / weak passwords, unpatched software, and misconfigured security settings. | It is not mentioned whether any controls are in place to secure | Possible | doomsday | Extreme | 3 |
| data on Disks | unauthorized access, and physical damage or theft / weak passwords, and a lack of encryption. | ----- | Unlikely | moderate | Medium | 16 |
| Customer information | identity theft, and unauthorized access, data breaches / weak passwords, misconfigured security settings, and lack of encryption. | customer profiles containing personal and private information should not be disclosed to other parties | almost certain | moderate | Extreme | 2 |
| Subnet | malware, and unauthorized access, hacking / weak passwords, misconfigured security settings, a lack of segmentation. | **a single subnet is used for all devices in all monitoring stations.** | possible | Minor | Medium | 15 |
| web application | malware, and unauthorized access, hacking / weak passwords, misconfigured security settings, unpatched software | data is transmitted through a published web application over the Internet | possible | Moderate | High | 9 |
| Internet connection | malware, and unauthorized access, hacking / weak passwords, misconfigured security settings, a lack of encryption | --- | possible | Insignificant | Low | 17 |
| VPN | malware, and unauthorized access, hacking / weak passwords, misconfigured security settings, a lack of encryption | employees and third parties have VPN access | possible | Insignificant | Low | 18 |

For every point the first part means the Threat and the second part after the / means the Vulnerability

**Part C**

Suggest (given the notes above) the possible controls/countermeasures initially used by the company to protect their asset.

|  |  |  |
| --- | --- | --- |
| Asset name | Suggested countermeasure | How can the suggested countermeasure protect the asset? |
| endpoints | Implement strong passwords, and device encryption, and access controls and apply two-factor authentication to secure endpoints. | can aid in preventing unwanted access to devices, provide improved security due to updated hardware and software, and be used to identify and defend against malware and other threats. |
| servers | Implement environmental controls (humidity and temperature controls) and updated software, and regularly patched to secure the servers | Locks and regularly patched and updated software help to prevent unauthorized access and protect against vulnerabilities and secure the servers, and temperature and humidity controls help equipment reliability by improving reliability and extending equipment lifespan, Energy efficiency by reducing energy consumption by preventing overcooling, and data protection by protecting the data and ensuring data integrity. |
| storage devices | Implement access controls, and encryption, and secure protocols when transferring data to and from it to secure storage devices. | Can help to protect it from being accessed by unauthorized parties, protect it from being intercepted by malicious parties, and ensure that only authorized users can access the data on the storage devices. |
| cables | Secure cables by using one of these or more: Physical locks (cable locks or cable ties), Cable trays or conduit, cable covers, secure, encrypted cables, or access controls | Physically secure making it more difficult for unauthorized parties to access them and the encrypted ones it protects the transmitted data |
| networking devices | Implement proper configuration (firewall and VPN) and access controls, and updating software, and regularly patching to secure it. | Properly configured VPN and firewall settings could help to prevent unauthorized access to warmaksan network. And the update/patch should help to address the vulnerabilities. |
| cloud infrastructure | Implement appropriate controls like a reputable cloud provider with strong security controls and Secure data transmission protocols, and evaluate the reliability and security carefully of the cloud provider | Can help to protect data and services stored in the cloud, and data transmitted over the Internet. |
| Monitoring stations | Implement appropriate security controls and segmentation the network into separate subnets for each subnet, and access controls and authentication procedures. | Helps to prevent unauthorized access to monitoring stations, and segmenting helps to prevent unauthorized access to sensitive data. |
| Data center | Implement environmental controls (humidity and temperature controls) and physical security controls (Locks), access controls, to secure it. | Locks and fingerprints Help prevent unauthorized access to networking devices and servers, and temperature and humidity controls help equipment reliability by improving reliability and extending equipment lifespan, Energy efficiency by reducing energy consumption by preventing overcooling, and data protection by protecting the data and ensuring data integrity. |
| Application / Operating system | update the Applications and the operating system to prevent vulnerabilities and regularly patch | Updating the software and the operating system and regular patching help to protect against threats and address vulnerabilities |
| Security software | Regularly update | To ensure it is effective at protecting against threats, it could protect and detect any threats and malware. |
| Backup and recovery software | Implement a recovery plan and procedures, robust backup, regular testing, and updating backup | To ensure the availability of the data, and it can be recovered in the event of a disaster. |
| data on Disks | implementing encryption and access controls. | It helps to protect data stored on the disks from being accessed by unauthorized parties, and it restricts access to authorized users only. |
| Customer information | access controls and Implement encryption, and Authentication procedures | help to protect customer information and prevent unauthorized access to personal and private information. |
| Subnet | Implement appropriate security controls and segmentation for each subnet. | It helps to prevent unauthorized access to sensitive data. |
| web application | Implement secure authentication, encryption, and access controls, and regularly patch and update the application to secure it. | It protects data transmitted through the application from being accessed by unauthorized parties. And helps to address vulnerabilities. |
| Internet connection | using VPN / Firewall / secure Wi-Fi and router and Implementing appropriate security controls to protect it. | Protect data transmitted over the Internet from being accessed by unauthorized parties. |
| VPN | Implement proper configuration and access controls to secure the VPN | Help to prevent unauthorized access, and compromised accounts. |

**Part D**

Recommend ways to improve Warmaksan's IT security via:

**A**

Describe and assessing different security controls that could be applied to protect the most critical assets (customers & business-critical data)

1. Strong access controls can be implemented to help ensure that only authorized workers and staff have access to customer and business-critical data. Implementing user activity monitoring tools and regularly assessing multifactor authentication could be part of this.
2. Putting in place a disaster recovery and business continuity strategy to make sure that data and vital systems can be recovered in the event of an emergency, security breach, or other disruption, and testing it frequently to be ready in case it does.
3. Use encryption to safeguard vital corporate data and consumer information. This could aid in preventing its disclosure or illegal access, including for both transmitted and at-rest data.
4. Using physical security measures, such as CCTV, locked doors, and alarm systems, to prevent unwanted access to data centers, servers, and other locations
5. Implementing firewalls, VPNs, intrusion detection methods, and other network security checks.

**B**

Explain data protection processes and regulations that might enhance Warmaksan's IT security.

1. AES or RSA are simply a couple of encryption technologies that may be used to implement data encryption. This can be done for both on-premises and cloud-based data.
2. Warmaksan should have a plan in place to respond to security incidents in a timely and efficient manner and to lessen their negative effects on the business. Procedures for locating, containing, and resolving security incidents should be part of this. For instance, this could entail deciding which people is best suited to handle the situation, laying out the steps to be done to contain it, and developing protocols for informing the right authorities about the issue.
3. Strong access controls can be achieved by limiting data access to people who require it for their work responsibilities and by routinely evaluating.
4. Warmaksan's data may be simply and rapidly retrieved in the case of a data loss or disaster by putting into place a reliable data backup and recovery plan. Offsite storage, routine backups, and disaster recovery testing may all be part of this.
5. The protection of consumer personal data, including names, addresses, and financial information, can be achieved by implementing data privacy rules and processes. This could involve setting up suitable data access restrictions, such as multifactor authentication and role-based access controls, and encrypting sensitive data both in transit and at rest.
6. There can be particular data protection laws that Warmaksan must follow depending on where its operations are located. For instance, observing data protection laws like HIPAA, GDPR, CCPA, and others places tight restrictions on how personal data is handled and protected. As well as assisting in ensuring that Warmaksan's IT security complies with all applicable legal and regulatory standards. This can entail putting in place the necessary data protection safeguards, like incident response strategies, data encryption, and data access controls.
7. The comprehensive data privacy law known as the General Data Protection Regulation (GDPR) went into effect in the European Union in 2018. It controls how EU residents' personal data is handled and has significant ramifications for any businesses that handle this kind of data. Companies are required by GDPR to take reasonable technical and organizational steps to protect personal data, designate a Data Protection Officer, notify individuals of data breaches within 72 hours, and grant them certain rights, such as the ability to access, correct, and delete their personal data, and Since Warmaksan processes personal data, it is crucial that it abide by GDPR because of its legal responsibilities to protect such data. Regardless of matter where the business processing the data is located, GDPR is applicable to any processing of personal data. As it is likely to process the personal data of EU individuals, including employees, customers, or other sorts of personal data, Warmaksan should take the necessary precautions to ensure that it is GDPR-compliant. It encompasses everything from risk management and vulnerability scans to firewalls and third-party due diligence. GDPR compliance will help to protect the sensitive personal data that Warmaksan manages and aid to avoid large fines and penalties in case of any data breaches.

**C**

Analyze the IT security audit and its impact on Warmaksan IT security.

**IT Security Analysis**

Several solutions can be put into place to make the situation better, starting with the endpoint devices in the network that lack protection. To protect against malware and other malicious software, one way is to install antivirus software on all endpoint devices. By limiting incoming and outgoing traffic, firewall configuration on these devices can also help to safeguard the network. Implementing numerous subnets, such as one for each continent, is another way to address the problem of heavy traffic produced by all devices being connected to a single subnet. By doing so, congestion can be lessened, and overall network performance can be enhanced.

The Warmaksan employees' existing password policy is another issue that has to be addressed. A new password policy that mandates stronger and more difficult passwords can be issued to address the numerous problems with this one. Additionally, only personnel who genuinely need remote access to the data center should have it, and anyone using VPN access for support purposes should be held responsible for any data loss.

It is also possible to increase the security of the servers and networking equipment inside the data center. Installing security measures like digital fingerprints or other biometric authentication techniques to safeguard the door to the data center is one way to handle this problem. In order to stop servers from breaking down, the server room's temperature and humidity should also be regularly monitored and managed.

By adhering to accepted guidelines and recommended procedures for IT security, auditing problems within the system can also be resolved. This could entail carrying out appropriate incident response procedures and disaster recovery plans, as well as conducting routine security audits and vulnerability assessments.

Overall, while Warmaksan's infrastructure is competent for securing client data, the measures that are currently in place are insufficient to address future potential data loss or assaults. The above-mentioned recommendations can greatly enhance the security of Warmaksan's IT infrastructure.

**Security Audit Impact**

The organization's overall IT security may be significantly impacted by the security audit for Warmaksan. The audit can show where the security architecture is currently weak and vulnerable and offer suggestions for improvement. To better safeguard against illegal access, this can involve putting in place stricter network access rules, encrypting sensitive data, and upgrading password policies. The audit can also assist Warmaksan in assessing and enhancing their security procedures to make sure they are compliant with current laws and standards.

A security audit can also assist Warmaksan in preparing for upcoming security problems, which is a significant advantage. The organization can create and implement plans to reduce or stop threats by recognizing potential risks and vulnerabilities. This may involve putting incident response plans into place, educating staff members about security best practices, and spending money on security tools like intrusion detection and prevention systems.

The audit will also assist Warmaksan in holding any responsible parties accountable. An audit can benefit the business, particularly as it transitions to the cloud and more third parties become recognized for stealing information and being unreliable. It can also hold these parties accountable for their activities and prevent them from stealing.

In conclusion, Warmaksan may find that a security audit is a useful tool for enhancing the overall security of their IT systems and safeguarding private information from intrusions and breaches. Additionally, it can assist the company in preparing for potential dangers and hold any responsible parties accountable.

Analyze the results of the IT security audit and prioritize any identified vulnerabilities or risks based on their potential impact on Warmaksan's IT security, assess the security of the data center, including physical security, access controls, and environmental controls, and the other devices, networks, applications to ensure the safety and availability of the data, understand and evaluate the existing security controls in place and their effectiveness to mitigate the identified risks, identifying any gaps in the existing security controls and assessing the potential impact on Warmaksan IT security, and evaluate warmaksan's security monitoring capabilities, evaluating the success of the incident response, disaster recovery, and business continuity plan to ensure that they are sufficient to handle security incidents and data breaches, and Implementing it will ensure that, in the event of an incident, the system can be rapidly restored. To ensure that all employees understand the value of IT security and how to protect the system from attacks, identify any employee-related hazards, such as a lack of security awareness and training. Then, conduct regular security awareness and training for all employees. To guarantee the availability of data in the event of an emergency, regularly back up your data. For all accounts and devices, implement a multi-factor authentication system. Limit VPN access to the data center to authorized people only by implementing suitable access controls and monitoring procedures, To separate various devices and subnets, use network segmentation. Utilize security monitoring technologies to quickly identify and address security incidents.

**Part E**

Review the risk assessment procedures in Warmaksan.

**1**

It is necessary to compare the present permissible risk level to them, To make sure it is in line with industry norms and laws, and check the potential effects of the hazards found throughout the risk assessment process to see if they match the degree of risk that is now deemed acceptable, determine Warmaksan's risk tolerance and confirm that the acceptable risk level is consistent with the aims and objectives of the company, and develop a strategy to reduce or eliminate any risks that are more than the acceptable risk level, and it should be reviewed frequently and updated as appropriate to keep the acceptable risk level current and in line with Warmaksan's risk profile and goals, and Inform the board of directors, management, and all other Warmaksan stakeholders of the acceptable risk level.

**2**

1. Analysis of the Business impact and operational effects of security incidents on Warmaksan operations.
2. Penetration testing: Warmaksan's systems, networks, and data are subjected to it, which simulates a cyber-attack in order to find weaknesses and possible points of entry for attackers.
3. The social engineering evaluation tests Warmaksan's sensitivity to these kinds of attacks as well as the staff's ability to spot and report such ploys by simulating social engineering attacks including phishing, fishing, and baiting.
4. The risk management assessment's: The main objective is to examine Warmaksan's risk management procedures and pinpoint opportunities for development.

**3**

1. identifying and cataloguing Warmaksan's essential resources, such as its staff, systems, data, and networks.
2. Identifying potential internal and external risks, as well as natural and man-made disasters, to Warmaksan's security
3. assessing Warmaksan's current security measures and locating any gaps or holes, and estimating how each identified threat would affect the vital resources of Warmaksan, and calculating the likelihood that a specific threat will materialize, and Putting risks in order of importance based on likelihood and potential impact.
4. as a result, creating a strategy to reduce or eliminate the risks that have been identified, including putting new security controls in place, enhancing current controls, and creating strategies for incident response and catastrophe recovery.
5. Putting the plan into action, keeping an eye on it, and periodically evaluating and revising the plan will ensure that it remains relevant and efficient in managing the risk profile of the firm.

**4**

The level of danger that Warmaksan is willing to bear in its activities is the acceptable risk level. It is a crucial component of the risk management process because it enables Warmaksan to make well-informed decisions about how to allocate resources to minimize risks. It is a measure of the amount of risk that Warmaksan is ready to tolerate in order to achieve its goals and objectives. By examining a risk's potential impact, likelihood of occurrence, and cost of risk mitigation, the acceptable risk level is established.

After establishing the acceptable risk level, Warmaksan can put controls in place to reduce risks that are higher than the acceptable risk level. Implementing security measures like firewalls and intrusion detection systems may fall under this category.

Additionally, it might alter as the danger environment and the Warmaksan's risk profile vary over time. As a result, Warmaksan should periodically examine and adjust their acceptable risk level to make sure it remains relevant and in line with their goals and objectives.

**Part F**

Explain how you can benefit from an appropriate risk management approach or ISO risk management methodology by summarizing it and highlighting its application in the IT security of this project.

Warmaksan can gain from a suitable risk management strategy or ISO risk management methodology by offering a planned and methodical approach to detecting, evaluating, and mitigating security risks to the company's data and systems. This comprises:

Warmaksan and others can benefit from identifying potential risks. This entails identifying possible security threats and weaknesses that may jeopardize the privacy, availability, and integrity of the company's data and systems. For instance, if an unauthorized person acquires access to the cloud storage account, Warmaksan may notice a potential danger that the client data it has stored there could be compromised.

Determining the impact and likelihood of risks, The likelihood and significance of each prospective risk, should be evaluated when potential risks have been identified. As a result, the risks that need to be addressed will be prioritized, and the necessary level of mitigation will be determined. Because client data is considered private and is protected by law and regulations, it may be concluded that the likelihood of an unauthorized person accessing the cloud storage account is significant owing to weak passwords, and the impact may be severe.

Mitigating risks, The right steps should be done to reduce or eliminate risks after determining their likelihood and impact. This may entail putting in place security measures like firewalls and VPNs as well as creating incident response and reporting protocols, Warmaksan, for instance, might put in place password rules, multi-factor authentication, and regular security audits to make sure that the cloud storage account is safe and that customer data is safeguarded.

To ensure that risks are handled successfully and to spot any potential new threats, regular monitoring and review of the risk management process is crucial. For instance, Warmaksan might frequently audit its security measures and evaluate and update its risk management guidelines and policies to make sure they are current and efficient.

ISO 31000 is a global risk management standard. By following the guidelines outlined in the standard, Warmaksan can make sure that it has a reliable and effective risk management strategy and can better preserve the security and integrity of its data and systems. The standard provides a framework for identifying, assessing, and managing risks and contains best practices for risk management processes and procedures. By conforming to the ISO 31000 standard, Warmaksan may ensure that risks are managed consistently, uniformly, and in compliance with international standards for risk management. The organization may also more successfully demonstrate to regulators, auditors, and clients that it is adopting a proactive and all-encompassing strategy to reducing risks to its systems and data by putting the standard into practice.

Improved risk identification: The structured method to risk identification provided by ISO 31000 can assist Warmaksan in finding risks that may have previously gone unnoticed. Risks associated with new technology, modifications to the corporate environment, and emerging dangers might all fall under this category.

Consistent risk assessment: The ISO 31000 standard offers instructions for determining the possibility and consequences of risks, which Warmaksan can use to make sure that it is accurately and consistently evaluating the risks it encounters. This may enhance the efficiency of risk reduction measures.

Improved communication and collaboration: The ISO 31000 standard encourages communication and cooperation across various organizational departments and functions, which can assist Warmaksan make sure that all pertinent stakeholders are involved in the risk management process. This may enhance the risk management program's overall efficacy.

Better alignment with organizational goals: ISO 31000 offers advice on how to match risk management initiatives with a company's overarching corporate goals. This can assist Warmaksan in making sure that its risk management initiatives are in line with its corporate goals and objectives, which can enhance the program's overall performance.

Improved compliance: The ISO 31000 standard for risk management is a globally recognized one, and adhering to it can help Warmaksan show regulators, auditors, and clients that it is adopting a proactive and rigorous approach to controlling risks to its data and systems.

ISO 31000 outlines a set of principles for managing risk. These principles include a focus on the continual improvement of risk management processes, the involvement of relevant stakeholders in the risk management process, and a transparent and systematic approach to risk management.

Principles: The cornerstone for efficient risk management is provided by the ISO 31000 principles. A dedication to risk management, the incorporation of risk management into decision-making, and the consistent use of risk management are some of these principles. These principles can be put into reality in the context of Warmaksan's IT security by committing to routinely assessing and addressing potential risks, including risk management factors in all IT security decisions, and consistently implementing risk management procedures across the business.

The framework of ISO 31000 includes a process for identifying, assessing, and treating risks. This process includes steps such as risk identification, risk analysis, risk evaluation, and risk treatment. Within this framework, organizations are encouraged to consider both the likelihood and potential impact of risks and to develop a risk management plan that is appropriate for their specific needs.

Framework: The essential elements of a successful risk management system are described in the ISO 31000 framework. This include recognizing and evaluating risks, addressing risks, and keeping an eye on and evaluating the success of risk management. This methodology can be used in the context of Warmaksan's IT security by routinely identifying and evaluating potential IT security risks, putting in place steps to lessen or eliminate these risks, and continuously analyzing and monitoring the efficacy of these efforts.

The process of ISO 31000 also includes ongoing monitoring and review of risk management activities to ensure that they remain effective over time. This includes regular reviews of the risk management plan, as well as the collection and analysis of data on the performance of risk management activities. Organizations are also encouraged to involve relevant stakeholders in the risk management process, including employees, customers, and other stakeholders who may be impacted by risks. Overall, the standard provides guidance for organizations on how to establish, implement, maintain, and improve a framework for risk management.

Process: The procedures that should be done to successfully manage risks are described in the ISO 31000 process. establishing the context, detecting risks, evaluating risks, addressing risks, and monitoring and evaluating the success of risk management are all included in this. This process can be applied to Warmaksan's IT security by establishing the organization's unique IT security context, identifying potential risks to IT security, evaluating the likelihood and impact of these risks, putting measures in place to reduce or eliminate these risks, and continuously reviewing and monitoring the efficacy of these measures.

**Part G**

Discuss, in detail, the security impact of any misalignment of IT security with Warmaksan policy and recommend how to maintain their alignment.

It may begin with inadequate security for important data, thus Sensitive client data may be at danger of being accessed or compromised by unauthorized individuals if IT security is not correctly matched with Warmaksan's data protection policies. This could result in data breaches and violations of data privacy laws and regulations, and can be resolved by Review and update security policies and procedures on a regular basis. Regularly reviewing and updating the policies and procedures to make sure they are current and effective is important, as is communication and collaboration. It is crucial that IT security and other relevant departments, such as HR, Legal, and Compliance, work together to make sure that policies and procedures are aligned and effective.

Second, the risk of security events has increased, hence Warmaksan may not be able to efficiently respond to and mitigate security issues if IT security is not properly aligned with its incident response and reporting rules. This could raise the danger of security lapses and data loss, so risk management is required. To discover and assess potential security risks and vulnerabilities, conduct security risk assessments on a regular basis. The alignment of IT security measures with the company's risk management strategy and policies will be improved as a result.

The third, violation of legal requirements and industrial regulations: Warmaksan may not be in compliance with data privacy and security laws and regulations if IT security is not properly coordinated with the company's compliance policies. We must perform a Compliance by ensuring that IT security measures and procedures are in line with industry regulations and laws related to data privacy and security. Failing to do so could result in significant fines and penalties for the business, or customers and third parties could easily sue Warmaksan. This can be accomplished by routinely evaluating and revising compliance policies and processes, carrying out routine compliance audits, and regularly training workers on security to ensure that they are aware of the organization's security policies and procedures ensuring that they are knowledgeable about potential dangers and effective ways to reduce them.

**Part H, I, J**

**Warmaksan Policy**

**Policy 1:** Backup data Policy

**What is it and its importance:**

It is a collection of rules that specify how a company should make and keep backups of its crucial data to make sure that it can be recovered in the case of a disaster, data loss, or hack. Because each branch's data will be uploaded to the system, a backup data policy is crucial to Warmaksan because it is responsible for safeguarding crucial data and making sure that it can be restored in the event of a disaster or data loss.

**Scope:**

Regarding the Warmaksan data centers and devices' data

**Policy:**

1. Use Grandfather-Father-Son Method
2. To ensure that backups can be restored in the case of a disaster or data loss, they must be kept in various locations, including off-site.
3. It's important to frequently test backups to make sure they can be successfully recovered.
4. Only a select few personnel, such as the admin, should be given access.

**Evaluate the used tools in the policy:**

The software is helpful for having a backup copy, making it simple to retrieve the data when you need to, and protecting the data from harm because it is stored in a different nation. However, it is harmful if your data is sensitive, and you didn't safeguard it properly.**Policy 2: Remote access policy.**

**What is it and its importance:**

It is a set of rules and procedures that regulate how contractors, employees, and outside vendors access the company's network and systems from remote locations, It is crucial for Warmaksan as it aids in safeguarding sensitive data and systems from unauthorized access as well as ensuring compliance with laws and industry standards relating to data privacy and security.

**Scope:**

everyone who needs remote access to the company's network and systems, including contractors, employees, and third-party vendors.

**Policy:**

1. All remote access connections must require multifactor authentication.
2. Only authorized users with a legitimate business need and access will be allowed to remotely access the company's network and systems.
3. Remote access connections need to be managed and watched over by firewalls and intrusion detection systems.
4. The main remote access techniques will be VPN and remote desktop protocols.
5. All data sent over remote access connections must be encrypted, to prevent unapproved access and exposure.

**Evaluate the used tools in the policy:**

multiple-factor verification and VPN to guard against unwanted access and data breaches, it has strong security measures and access controls and encryption.

**Policy 3: Firewall and VPN policy**

**What is it and its importance:**

It serves as a defense against unwanted access and data breaches for a company's network and systems. A VPN enables users to securely access a company's network from remote locations, reducing the risk of security breaches and data loss while ensuring that the company's data and systems are always accessible to authorized users. A firewall is a network security system that monitors and controls incoming and outgoing network traffic.

**Scope:**

anybody who needs access to the company's network and systems, including contractors, third-party providers, and employees.

**Policy:**

1. Only necessary inbound and outbound traffic should be permitted by the firewall.
2. Firewalls should be set up to automatically block all traffic and only permit that which has been specifically authorized.
3. VPN should be set up to employ reliable authentication and encryption protocols.
4. Only authorized workers should be able to access the firewall and VPN.

**Evaluate the used tools in the policy:**

VPNs: In addition to enabling warmaksan to conceal confidential information, it's useful in safeguarding remote connections in other ways.

Firewalls: The network is protected by it, which stops unauthorized and undesired traffic from entering. Efficient in preventing illegal network access.

**Policy 4: Third party policy**

**What is it and its importance:**

It is a set of rules and processes that control how to access and utilize a VPN and how much data is exchanged with outside parties (contractors, vendors, suppliers), Additionally, it assists Warmaksan in keeping its systems and sensitive data accessible to authorized users and guarding against unwanted access.

**Scope:**

all external parties that require remote access to the company's network and systems.

**Policy:**

1. Suppliers and third-party vendors are required to utilize the company's VPN client and adhere to its security settings.
2. When connecting to the company's VPN, third-party vendors and suppliers must use robust encryption and authentication procedures.
3. Only authorized employees should have access to the company's VPN.

**Evaluate the used tools in the policy:**

VPNs: In addition to enabling warmaksan to conceal confidential information, it's useful in safeguarding remote connections in other ways.

**Policy 5: General Data Protection Regulation**

**What is it and its importance:**

The comprehensive data privacy law known as the General Data Protection Regulation (GDPR) went into effect in the European Union in 2018. It controls how EU residents' personal data., help to protect the sensitive personal data that Warmaksan manages, and it is crucial that it abide by GDPR because of its legal responsibilities to protect such data

**Scope:**

all Warmaksan contractors, third-party providers, and employees who operate with personal data belonging to EU residents.

**Policy:**

1. The GDPR mandates that all personal data of EU citizens be routinely backed up using software that complies with its specifications.
2. Ensuring the security of the data backup program and that the data is shielded from unauthorized access.
3. Warmaksan will only keep personal information about EU residents as long as it's required for the specific reason it was obtained, after which it will be safely deleted.
4. Warmaksan will hire a DPO, to monitor the application and enforcement of this policy, as well as GDPR compliance.

**Evaluate the used tools in the policy:**

Software for data backup: Because of the usage of the cloud system, accessing the files through the backup program is quick and simple. The application will restore them immediately in the event of disasters, such as power failures during the backup process, ensuring that they are not lost.

**Policy 6: Clean desk policy**

**What is it and its importance:**

it is a set of guidelines that dictate how employees should maintain their workspaces to ensure the security and confidentiality of sensitive information. And what materials should be left out in the open and how to properly secure sensitive documents, The importance of a Clean Desk Policy to Warmaksan lies in the fact that it is responsible for protecting sensitive information, including the personal data of customers.

**Scope:**

All Warmaksan employees

**Policy:**

1. When not in use, all sensitive materials, including written papers, digital files, and other resources, must be adequately secured. This includes adopting other secure storage techniques, such as locking them in a cabinet or drawer, as necessary.
2. A password or other secure login technique must be used to protect all electronic devices, including computers, tablets, and smartphones.
3. Employees should avoid putting sensitive papers out in the open and should keep the amount of private information shown on their desks and workstations to a minimum.
4. At the end of each workday, all employees are required to tidy up and organize their desks, making sure that all sensitive materials are properly secured and securely stored and that their workstations are left in a tidy condition.
5. Keep the amount of sensitive information displayed on their desks and workstations to a minimum and to avoid leaving such materials out in the open.

**Evaluate the used tools in the policy:**

Employee training: It will educate staff members on how to handle data while adhering to the CIA triad of confidentiality, integrity, and availability. In order to prevent unauthorized access, the possibility of data modification during a transfer, and take the necessary precautions.

**Policy 7: Password policy**

**What is it and its importance:**

In order to guarantee the security of corporate data and systems, it is a set of rules that specify how employees should establish and manage their passwords. The policy provides detailed instructions on how employees should generate and store their passwords, and A password policy is crucial to Warmaksan since it is in charge of safeguarding confidential data and business processes. Reduced risk of unwanted access to warmaksan information is made possible by a password policy.

**Scope:**

All Warmaksan workers who have access to corporate information and systems, including contractors, third-party vendors, and employees.

**Policy:**

1. All workers are required to create secure passwords that are at least 8 characters long and contain a mix of uppercase, lowercase, numerals, and special characters.
2. Passwords must be changed by employees at least every 45 days.
3. Employees shouldn't use passwords that can be easily guessed, including their name or address.
4. Passwords shouldn't be written down or shared by employees with others.

**Evaluate the used tools in the policy:**

Employee training: It will educate staff members on how to handle data while adhering to the CIA triad of confidentiality, integrity, and availability. In order to prevent unauthorized access and the possibility of data modification during a transfer, they will take the necessary precautions.

**Part K**

A discussion of the roles of stakeholders in the Warmaksan to implement security audit recommendations.

It is crucial to involve various stakeholders who play different roles in the organization in the implementation of security audit recommendations at Warmaksan. This way, they will be aware of their exact roles and what needs to be done to create a safe workplace and a wonderful environment where our employees can work and be as productive as possible. The following is a summary of some of the crucial stakeholders' roles in putting security audit recommendations into practice:

Management plays a crucial role in the implementation process and is in charge of deciding on warmaksan's overall strategy and direction, as they are responsible for providing the necessary resources, support, and money, and direction for the security audit recommendations to be carried out effectively. They also need to establish a clear communication channel for the stakeholders and ensure that the recommendations align with the company's overall strategy and objectives, they are also in charge of making sure the company complies with all applicable laws and regulations.

IT Officers have a significant responsibility in the implementation of security audit recommendations. They are responsible for ensuring that the recommendations align with the company's IT policies and procedures. They also need to evaluate the technical feasibility of the recommendations and ensure that they are implemented correctly.

Risk Owners are responsible for identifying and managing risks within the company. They play a vital role in the implementation of security audit recommendations as they need to ensure that the recommendations align with the company's risk management policies and procedures. They also need to identify potential risks that may arise from the implementation of the recommendations and take the necessary steps to mitigate them.

Facility and security teams are responsible for ensuring the physical security of the company's facilities and assets. They play a vital role in the implementation of security audit recommendations, as they need to ensure that the recommendations align with the company's facility and security policies and procedures. They also need to ensure that the physical security measures are in place to protect the company's assets.

Risk and Compliance teams are responsible for ensuring that the company is in compliance with relevant laws, regulations, and standards. They play a vital role in the implementation of security audit recommendations, as they need to ensure that the recommendations align with the company's compliance policies and procedures. They also need to ensure that the company is in compliance with relevant laws, regulations, and standards.

Information Security Officer (ISO): The ISO is in charge of ensuring that the organization's information systems and networks are generally secure. By creating and putting into practice security policies and procedures and managing day-to-day security operations, they play a crucial part in putting security audit recommendations into practice. They are also in charge of making sure the company complies with all applicable laws and regulations.

IT department: The IT department is in charge of running and maintaining the organization's networks and information systems on a daily basis. By establishing technical controls and processes and ensuring that the organization's systems and networks are configured in accordance with best practices, they play a crucial role in putting security audit recommendations into practice.

Legal department: The legal department is in charge of making sure that the company complies with all applicable laws and regulations. They analyze the suggestions and identify any legal or regulatory obligations that must be met, which is one of their significant contributions to the implementation of security audit recommendations.

Department of human resources (HR): The HR department is in charge of managing the workforce of the company, including recruitment, development, and training. By creating and implementing security awareness training programs for employees and making sure that they are aware of the organization's security policies and procedures, they play a crucial part in putting security audit recommendations into practice.

Third-party suppliers: By offering the tools, services, and support required for the execution of security measures, third-party vendors can contribute to the implementation of security audit recommendations. They should be informed of the organization's security expectations and requirements and held responsible for upholding them. It's critical to assess the suppliers' security precautions and make sure they abide by the organization's security rules and regulations.

Customers: By offering feedback on security measures and ensuring that their personal data is handled safely, customers may play a critical role in putting security audit recommendations into practice.

Auditors: By giving an unbiased assessment of the organization's security posture and highlighting areas for improvement, auditors play a crucial role in putting security audit recommendations into practice. They must take part in the implementation procedure to make sure the suggestions are carried out correctly and to offer continual supervision.

All parties must cooperate and work together to guarantee that the security audit recommendations are carried out. The effectiveness of the implementation depends on open communication and a shared awareness of the risks and obligations. The management should design an open and explicit approach for carrying out recommendations and frequently assess the implementation's progress and outcomes.

**Recourses**

(no date) *https://circle.cloudsecurityalliance.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=75f04c8e-e2fe-4c99-bec1-2579b08ef89f*. rep.

(no date) *Inicio*. Available at: https://icontec.isolutions.iso.org/obp/ui#!iso:std:iso:20318:-1:ed-1:v1:en (Accessed: January 30, 2023).

Compliance, K.Y. (2022) *What are GDPR Technical and organisational measures?*, *Know Your Compliance Limited*. Available at: https://www.knowyourcompliance.com/gdpr-technical-organisational-measures/ (Accessed: January 30, 2023).

Daniels, J. (2021) *Think GDPR only means reporting data breaches within 72 hours? think again*, *BetterCloud*. Available at: https://www.bettercloud.com/monitor/data-breaches-within-72-hours/ (Accessed: January 30, 2023).

*ISO - International Organization for Standardization* (no date). Available at: https://www.iso.org/ (Accessed: January 29, 2023).

*What is GDPR, the EU's new Data Protection Law?* (2022) *GDPR.eu*. Available at: https://gdpr.eu/what-is-gdpr/ (Accessed: January 30, 2023).