

**Security**

**10203280**

**D/618/7406**

**Section (2)**

**Warmaksan**

**Submitted to**

Eng. Sami Al Mashaqba

**Submitted on**

January 31st, 2023

**Submitted by**

Marwan Tareq Shafiq Al Farah

**Student ID**

21110011

**Fall 2022 - 2023**

**Table of Content**

[***Report*** 3](#_Toc125790976)

[**A.** **Most Critical Assets of Warmaksan's System** 3](#_Toc125790977)

[**B.** **Warmaksan System’s Possible Risks** 4](#_Toc125790978)

[**C.** **Possible Countermeasures initially used by Warmaksan to Protect their Assets** 9](#_Toc125790979)

[**D.** **Recommendations to Improve Warmaksan's IT security** 10](#_Toc125790980)

[**a.** **Description and Assessment of Different Security Controls** 10](#_Toc125790981)

[**b.** **Data Protection Processes and Regulations** 11](#_Toc125790982)

[**c.** **Analysis of the IT Security Audit and its Impact** 13](#_Toc125790983)

[**E.** **Revision of the Risk Assessment Procedures in Warmaksan** 13](#_Toc125790984)

[**F.** **Benefits from the ISO Risk Management Methodology** 14](#_Toc125790985)

[**G.** **Misalignment of IT Security with Warmaksan Policy** 15](#_Toc125790986)

[**a.** **The Security Impact of this Misalignment** 15](#_Toc125790987)

[**b.** **Recommendations on How to Maintain their Alignment** 16](#_Toc125790988)

[**H.** **Warmaksan’s Security Policy** 16](#_Toc125790989)

[**I.** **Justification of the Developed Security Plan** 17](#_Toc125790990)

[**J.** **Evaluation of the Suitability of the Tools Used in the Policy** 18](#_Toc125790991)

[**K.** **The Roles of Stakeholders in Implementing Security Audit Recommendations** 19](#_Toc125790992)

[***References*** 21](#_Toc125790993)

[***Security Policy*** 22](#_Toc125790994)

[***Student Declaration Form*** 27](#_Toc125790995)

# ***Report***

1. **Most Critical Assets of Warmaksan's System:**

As the Information Security Risk Officer for Warmaksan, it is crucial to protect the company's critical assets, including client data, the social networking site "Donzel," the datacenter and offices/branches, servers, networking devices, endpoint devices, the cloud infrastructure and software. These assets are essential for the success and reputation of the company and must be protected to ensure their confidentiality, integrity, and availability (CIA). The most critical assets of the Warmaksan system can probably be summarized in the following.

The endpoints within the offices, which include employee workstations, laptops, and any other device that can connect to the network are critical because they contain sensitive information and are used to access the company's network and resources. They also play a critical role in the day-to-day operations of the company.

All devices located in the subnet which include servers, routers, switches, and any other networking equipment that is connected to the network are essential for maintaining the company's network infrastructure and ensuring proper communication and access to resources for employees and customers.

Another critical asset is the data transmitted through the web app, which includes any data

that is being sent or received through the web application, such as customer information,

login credentials, and other sensitive data. This data is critical because it contains sensitive

information about the company's customers and is used to access the company's resources.

Customer profiles hosted on-premises, which include any customer information, such as personal details, contact information, and purchase history that is stored on the company's servers are also critical assets. This data is critical because it contains sensitive information about the company's customers and is used to access the company's resources.

Servers and networking devices which include any servers, routers, switches, and other networking equipment that is used to support the company's operations are essential for maintaining the company's network infrastructure and ensuring proper communication and access to resources for employees and customers.

Warmaksan's data in the datacenter, which includes any data that is stored on the company's servers, such as customer information, financial data, and other sensitive information is also a critical asset. This data is critical because it contains sensitive information about the company's customers and is used to access the company's resources.

Warmaksan's services and applications, which include any software or services that are used to support the company's operations, such as email servers, databases, and other applications are also critical assets. These services and applications are critical because they are used to access the company's resources and support the company's operations.

Accounts and data belonging to employees and clients, as well as any software or device requiring a password which includes any accounts, data, or devices that require a password for access, such as employee accounts, client accounts, and other software or devices. These accounts and data are crucial for the company's operations and their confidentiality and integrity must be maintained.

In terms of the CIA principles, these assets are critical because they are all important to the Confidentiality, Integrity and Availability of the company's information and systems. The endpoints, web app data, customer profiles, and company data all contain sensitive information that must be protected to maintain confidentiality. The integrity of this data is also important to ensure that it is accurate and can be trusted. The availability of these assets is critical to ensure that the company can continue to operate effectively and provide services to its customers.

1. **Warmaksan System’s Possible Risks:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | | 1. **Exploitation Consequences** | | | | | |
| **Insignificant** | **Minor** | **Moderate** | **Major** | **Catastrophic** | **Doomsday** |
| **Likelihood** | **Almost Certain** | Medium | Medium | High | High | Extreme | Extreme |
| **Likely** | Low | Medium | Medium | High | High | Extreme |
| **Possible** | Low | Low | Medium | Medium | High | High |
| **Unlikely** | Very Low | Low | Low | Medium | Medium | High |
| **Rare** | Very Low | Very Low | Low | Low | Medium | Medium |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Asset | Threat / Vulnerability | Existing control | Likelihood | Consequence | Level of Risk | Risk Priority |
| Servers and networking devices which includes any servers, routers, switches, and other networking equipment, located in the data center, that is used to support the company's operations | Physical security risk, potential for damage to hardware | Security guards, door without locks | Likely | Catastrophic | High | 1 |
| Warmaksan's services and applications which includes any software or services that are used to support the company's operations, such as email servers, databases, and other applications. | Increased attack surface, potential for exploitation of known vulnerabilities due to unpatched services and applications | All the previous patches and updates | Almost Certain | Major | High | 2 |
| Data transmitted through web app which includes any data that is being sent or received through the web application, such as customer information, login credentials, and other sensitive data | Unsecured data transmission, potential for data breach | The web app uses HTTP instead of HTTPS | Possible | Catastrophic | High | 3 |
| Warmaksan's data which includes any data that is stored on the company's servers, such as customer information, financial data, and other sensitive information | Increased attack surface, potential for unauthorized access or misuse of resources due to minor security procedures, and firewall and VPN misconfiguration | The existing security procedures and exciting firewall and VPN policies and configurations | Likely | Major | High | 4 |
| Endpoints within the offices which include employee workstations, laptops, and any other device that can connect to the network | These endpoints are vulnerable to attacks such as malware, phishing, and ransomware | Outdated antiviruses on these endpoints | Likely | Major | High | 5 |
| All devices located in the subnet which include servers, routers, switches, employee workstations, and any other networking equipment that is connected to the network | These devices are at risk of a single point of failure, which can make it easier for an attacker to compromise multiple devices at once | Firewall policies, IPS | Possible | Major | Medium | 6 |
| Warmaksan's data which includes any data that is stored on the company's servers, such as customer information, financial data, and other sensitive information | Increased attack surface, potential for unauthorized access or misuse of resources due to third parties with VPN access | Two-factor authentication, not encrypted VPN | Possible | Major | Medium | 7 |
| Warmaksan's data in the datacenter which includes any data that is stored on the company's servers, such as customer information, financial data, and other sensitive information | Insider threat, potential for unauthorized access or misuse of resources due to employees' VPN access | Two-factor authentication, not encrypted VPN | Unlikely | Major | Medium | 8 |
| Customer profiles hosted on-premises which includes any customer information, such as personal details, contact information, and purchase history that is stored on the company's servers | Unsecured data transmission, potential for data breach, unauthorized access to sensitive information | The data will be transferred using a web app that uses HTTP instead of HTTPS | Possible | Moderate | Medium | 9 |
| All software or devices that are being audited or used to audit (monitor and record) system and user activity for security and compliance purposes | Lack of monitoring the system and user activity, potential for malicious activity to go undetected or unaudited due to auditing issues | The existing auditing process | Rare | Major | Medium | 10 |
| Any accounts, data, or devices that require a password for access, such as employee accounts, client accounts, and other software or devices | Increased risk of unauthorized access, potential for password cracking or reuse due to the password policy issues | The existing password policy | Possible | Minor | Low | 11 |

Endpoints within the offices pose a risk to the confidentiality, integrity, and availability of the Warmaksan system due to a lack of proper security measures on devices. An attacker could potentially gain access to sensitive data or to the system through an unsecured device, leading to a confidentiality breach. They could also potentially modify or corrupt data, leading to an integrity violation. Additionally, the compromise of an endpoint device could result in a denial of service, leading to an impact on data availability. This threat, combined with a likelihood of occurrence, could result in a level of risk that is high.

The subnet used for all devices presents a risk to the availability of the Warmaksan system due to a single point of failure, thus if the subnet were to go down or become unavailable for any reason, all of the devices connected to it would also be affected which could result in a disruption of service. In addition, using a single subnet for all devices may make it easier for an attacker to compromise multiple devices at once, potentially leading to a confidentiality breach. This threat, combined with a likelihood of occurrence, could result in a level of risk that is medium.

The data that is transferred is subject to a confidentiality and integrity violations due to the data's unsecure transfer, along with the possibility of data breaches. For instance, if the data is transmitted over the Internet without the proper security measures, it may be compromised if it is intercepted by an attacker (man-in-the-middle). Additionally, there is a chance of illegal access or data modification if the database server or web application are not properly secured. The data in question is probably sensitive and falls under the category of customer privacy, which is protected by law and regulations such as the GDPR. As a result, it's crucial to protect this data's security both during transmission and storage. This threat, combined with a likelihood of occurrence, could result in a level of risk that is high.

Customer profiles hosted on-premises initially, means that the data is stored on a server that is located within the company's offices, then they are moved to the cloud which causes a risk to the confidentiality and integrity of this data if the profiles are not properly secured during the move from on-premises to the cloud. If the data is not properly encrypted or transmitted over a secure connection, it could be intercepted by an unauthorized party during transmission. There is also a risk of unauthorized access to the data if the profiles are not properly secured in the cloud. This threat, combined with a likelihood of occurrence, could result in a level of risk that is medium.

The physical security risk that the door to the data center, where the servers and networking devices are located, was easily opened and that the servers and networking devices are easily accessible by anyone along with the fact that the humidity and temperature inside the server room are poorly controlled, could compromise the availability of the Warmaksan system by potentially damaging the hardware of the datacenter, thus jeopardizing the clients' data and it could lead for the network to be inaccessible. Poor physical security of the data center could also allow unauthorized individuals to access the servers and networking devices, potentially compromising the data stored on the devices, leading to a continentality and integrity breach. This threat, combined with a likelihood of occurrence, could result in a level of risk that is high.

Employees with VPN access to the datacenter pose a risk to the confidentiality, integrity, and availability of the Warmaksan system if the VPN access is not properly secured. If an employee's VPN credentials are compromised, for example, an attacker could potentially gain unauthorized access to the data center and its resources, which could lead to a confidentiality breach or a compromise of the integrity of the data stored on the devices. This threat, combined with a likelihood of occurrence, could result in a level of risk that is medium.

Third parties with VPN access increase the risk to the confidentiality, integrity, and availability of the Warmaksan system due to an increased attack surface and the potential for unauthorized access or misuse of resources if the third party's VPN credentials are compromised, as well as the possibility that the VPN grants access to third parties that are not properly secured, which could lead to a confidentiality breach or a compromise of the integrity and availability of the data stored on the devices. This threat, combined with a likelihood of occurrence, could result in a level of risk that is medium.

A lack of security procedures along with some misconfigurations on network security devices such as firewalls and VPNs increase the risk to the confidentiality and availability of the Warmaksan system due to an increased attack surface and the potential for unauthorized access or misuse of resources. The lack of robust security procedures also increases the risk of a security breach or compromise of the Warmaksan system. If the firewall is misconfigured, it may not provide the intended level of protection and could potentially allow unauthorized traffic to pass through. Similarly, if a VPN is misconfigured, it could potentially allow unauthorized access to the network or compromise the confidentiality and integrity of data transmitted over the VPN. This threat, combined with a likelihood of occurrence, could result in a level of risk that is high.

Unpatched services and applications refer to software that has known vulnerabilities that have not been fixed with an update or patch and they present a risk to the confidentiality, integrity, and availability of the Warmaksan system due to an increased attack surface and the potential for exploitation of these known vulnerabilities by attackers to gain unauthorized access to the system or compromise its confidentiality, integrity, or availability. This threat, combined with a likelihood of occurrence, could result in a level of risk that is high.

Password policy issues increase the risk to the confidentiality and availability of the Warmaksan system due to the potential for unauthorized access and password cracking or reuse. For example, if passwords are not required to be complex or changed regularly, they may be more vulnerable to being guessed or cracked by attackers, and if passwords are allowed to be reused, an attacker who obtains a password for one account may be able to gain access to other accounts using the same password. This threat, combined with a likelihood of occurrence, could result in a level of risk that is low.

Auditing refers to the process of regularly reviewing and assessing the security of a system in order to identify potential vulnerabilities or weaknesses and ensure that the system is in compliance with security policies and regulations. Auditing issues, such as a lack of monitoring the system and user activity, present a risk to the confidentiality, integrity, and availability of the Warmaksan system due to the potential for malicious activity to go undetected or unaudited. This threat, combined with a likelihood of occurrence, could result in a level of risk that is medium.

The Warmaksan system is exposed to a variety of dangers that could jeopardize the asset's availability, confidentiality, and integrity. To guarantee the security and dependability of the system, these risks must be effectively addressed and reduced. Warmaksan can preserve the confidentiality, integrity, and availability of its crucial assets and fulfill its obligations to protect customer privacy and data by addressing these risks and putting in place the necessary procedures.

1. **Possible Countermeasures initially used by Warmaksan to Protect their Assets:**

Warmaksan has many possible controls/countermeasures that they initially used to protect their assets. For example, Warmaksan had previously installed antiviruses on all of their endpoints, but the problem is that Warmaksan had failed to keep these antiviruses up to date, therefore they became outdated, which makes their endpoints less secure and more susceptible for attacks.

Warmaksan also uses firewall policies to protect their subnet along with an Intrusion Prevention System (IPS), but the problem is that Warmaksan only uses a single subnet for all devices in all monitoring stations, which mean if the subnet where to get attacked or go down for any reason the whole subnet would go down, thus all devices connected to it would face a disruption of services due to a single point of failure.

Another existing control is that the data will be transferred to the cloud using a web app that uses HTTP instead of HTTPS, which increases the risk of security breaches, also, when customer profiles that are hosted on-premises get transferred to the cloud, they will be transferred using HTTP not HTTPS.

Warmaksan also uses doors that don't have locks on them in their datacenter, which increases the risk of many physical security breaches such as theft and vandalism, in contrary, Warmaksan's datacenter is heavily guarded by security guards which decrease the risk of these physical risks. Unfortunately, Warmaksan doesn't have any controls to regulate the datacenter's temperature and humidity.

As for the VPN connection, Warmaksan uses VPN that is not encrypted to help employees connect to Warmaksan's datacenter, as well as third parties that connect to the Warmaksan system, in contrary, these VPNs use two-factor authentication, thus to use the VPN you need to enter the password as well as another form of authentication such as an email, or a message to the user's phone.

Warmaksan's existing security procedures and policies are a part of the existing controls that Warmaksan utilizes, but the problem with these procedures is that they are very minimal and minor, and that they do not consider all the possibilities of threats, and they don't provide high security for the company. The firewall and VPN policies in Warmaksan are also a form of existing controls, but the problem with these controls it that they are misconfigured which can increase the risk of the exploitation of these vulnerabilities.

Warmaksan previously was very persistent of patching their system regularly and updating it, unfortunately, Warmaksan has stopped patching their services and applications which increases the risk of exploiting the known vulnerabilities, thus increasing the potential of attacks.

Warmaksan's existing password policy and auditing procedures is a form of an existing control used by Warmaksan, but the problem with it is that they have many issues, which increases the risk of attacks, due to the increased risk of unauthorized access, potential for password cracking, lack of monitoring the system and user activity, potential for malicious activity to go undetected or unaudited.

1. **Recommendations to Improve Warmaksan's IT security:**
2. **Description and Assessment of Different Security Controls:**

Some of the recommendations to improve Warmaksan's security is to:

* 1. Ensuring that all endpoint devices within the offices are properly secured by implementing a variety of security measures such as keeping the antiviruses up to date, using stronger passwords, as well as increasing employees' awareness on good security practices.
  2. Implementing controls such as proper network segmentation as it is vital to ensure the availability and security of the Warmaksan system. Network segmentation involves dividing the network into smaller, isolated segments (subnets), which can help prevent the compromise of multiple devices at once and limit the scope of an attack. Warmaksan could also implement a DMZ (demilitarized zone), add an extra layer of protection to protect the company's internal network.
  3. Implementing appropriate controls such as encryption and secure communication protocols to protect the data, whether it was the company's data or the new profiles that were hosted on-premises and then transferred to the cloud, during transmission, as well as access controls and strong passwords to protect the data in the cloud. It may also be necessary to regularly audit and test the security of the web application and database server to ensure the confidentiality and integrity of the data.
  4. Implementing appropriate controls such as strong physical security measures, including locks and security cameras, to protect the data center from unauthorized access. It is also important to ensure that the humidity and temperature inside the server room are properly controlled in order to protect the hardware and ensure the availability of the Warmaksan system. This may involve installing temperature and humidity control systems or monitoring devices to ensure that the conditions are within acceptable limits.
  5. Implementing appropriate controls such as strong passwords, two-factor authentication, and access controls to protect the VPN access for employees and third parties. It may also be necessary to regularly audit and monitor VPN usage to ensure that only authorized employees and third parties are using the VPN and that their access is appropriate.
  6. Properly configuring network security devices such as firewalls and VPNs to ensure that they are providing the intended level of protection. It is also important to implement robust security procedures and regularly audit and test the security of the system to ensure that it is adequately protected.
  7. Regularly patch and update services and applications in order to manage all of these risks, either by accepting, avoiding, transferring, or reducing them to mitigate the risks of these known vulnerabilities. This may involve installing updates or patches provided by the software vendor or developer or implementing workarounds or compensating controls to mitigate the vulnerabilities. It is also important to regularly audit and test the system to ensure that all services and applications are up to date and properly secured.
  8. Implementing a robust password policy that includes requirements for password length, complexity, expiration, and reuse. It may also be necessary to regularly audit and test the password policy to ensure that it is being followed and that passwords are being properly managed.
  9. Regularly audit the Warmaksan system and ensure that it is being properly monitored and tested for vulnerabilities. This may involve implementing tools and processes to monitor system activity, conduct regular security assessments, and identify and fix any issues that are discovered. It may also be necessary to regularly review and update security policies and procedures to ensure that they are adequate and in compliance with any relevant regulations.

1. **Data Protection Processes and Regulations:**

Data protection consists of all the measures taken to secure and safeguard vital data and information from being lost, corrupted, compromised, or accessed, used, disclosed without any authorization, while also enabling the option to restore the data to a usable state in the event that something were to happen to it (SNIA, 2020). Data protection is an umbrella term that involves traditional data protection methods (such as RAID, backup, and replication), data security (such as encryption, access control, and authentication), and data privacy (such as legislation, policies, and data governance) (SNIA, 2020). Some of the data protection process and regulations that might enhance Warmaksan's IT security include (Satori, 2022):

* 1. **Encryption:** to implement a data encryption strategy to safeguard data both during storage and transmission. Since encryption modifies data content using an algorithm that can only be undone with the proper encryption key, it can help prevent unauthorized access to data and safeguard its confidentiality and integrity. Even if data is taken, encryption makes it unreadable, preventing unauthorized access to your information.
  2. **Backup / Disaster Recovery / Data Loss Prevention (DLP):** to put in place methods for data backup and recovery to ensure that data can be retrieved in the case of a loss or disaster. it entails putting in place a range of procedures and tools that can be used to guard against data theft, loss, and accidental deletion, duplicate data and store it separately so it can be restored later and decide how an organization responds to a disaster or event that causes data loss or modification (such as a cyber-attack or natural disaster). In these procedures, a remote location containing copies of the protected systems is often set up, and operations are switched to those systems in the event of a disaster. These procedures are an essential tactic for maintaining business continuity when original data is lost, deleted, or corrupted.
  3. **Following data protection regulations:** one example of these regulations that Warmaksan might want to implement is the General Data Protection Regulation (GDPR). These guidelines and regulations specify precise standards for safeguarding private and personal information, deleting unneeded information when it is no longer necessary, and can assist Warmaksan to comply with all applicable laws governing data protection. The GDPR defines personal data as any information that can be used to identify a living individual, and it gives individuals more control over their personal data by giving them certain rights, such as the right to access, correct, and delete their data. Organizations that process personal data must also implement technical and organizational measures to ensure the security of that data.
  4. **Authentication and Authorization:** to implement procedures to guarantee that only authorized personnel can access data and systems in accordance with their roles or permissions. This may include implementing authentication techniques like passwords, biometric authentication, or two-factor authentication. Also, in order to restrict the actions that users are able to take on data and systems, it might also require putting in place access controls like permissions, access lists, and access policies.
  5. **Network Security Measures:** to put in place steps to secure the Warmaksan network and guard it against dangers like cyberattacks and unauthorized access. This may involve putting in place network security tools to monitor and manage incoming and outgoing network traffic, such as firewalls, intrusion prevention systems (IPS), and virtual private networks (VPN). Also, to secure data transmission and guard against data breaches, it is necessary to put security protocols in place like HTTPS.

1. **Analysis of the IT Security Audit and its Impact:**

An organization's information systems, networks, and security procedures are thoroughly examined during an IT security audit. By examining and testing the organization's security policies, procedures, and controls, examining system logs and network traffic, conducting vulnerability assessments, and reviewing the results, an IT security audit can assist Warmaksan in identifying potential weaknesses and areas for improvement, which will help to ensure the confidentiality, integrity, and availability of these systems. (Buckbee, 2020; Varghese, 2021; StandardFusion, 2022)

An IT security audit can significantly improve Warmaksan's IT security by giving the organization a thorough grasp of their present security status and the advantages and disadvantages of their current procedures. With the aid of this information, Warmaksan can prioritize their efforts to resolve any flaws or vulnerabilities found, identify areas for improvement, and deal with any issues that arise. An IT security audit can also assist Warmaksan in ensuring that they are in line with the data security laws and standards, such as the GDPR which could aid Warmaksan in protecting their clients' data, upholding their reputation, avoiding fines and other consequences for noncompliance by adhering to these standards. Finally, the IT security audit saves Warmaksan money by addressing any potential breaches before they occur.

In summary, an IT security audit can assist Warmaksan in identifying their weaknesses, evaluating the efficacy of these controls, recommending improvements for Warmaksan's IT security, ensuring compliance with security laws and standards like the GDPR, and finally resulting in an improved IT security status for Warmaksan.

1. **Revision of the Risk Assessment Procedures in Warmaksan:**

Risk assessment is the process of identifying, analyzing, and evaluating potential risks to the assets and resources of an organization. It entails determining the risks that could be posed to these assets, their likelihood of occurring, and the effects they might have if they did. The risk assessment procedure can assist Warmaksan in comprehending and prioritizing its risks so that it can put in place the necessary controls and mitigation strategies to lessen or eliminate those risks. (Lucidchart, 2020; CCOHS, 2021; Tajuddin, 2021)

After looking over Warmaksan's risk assessment procedures, it became apparent that the process was not being followed in an orderly and systematic way. It appeared that Warmaksan did not routinely review and update its risk assessment procedure to account for changes to the organization's assets, threats, and vulnerabilities. Because they are unaware of these risks and their extent, the organization may not be ready to deal with new or developing threats and may not be able to appropriately defend itself from them.

It is advised that Warmaksan adopt precise standards for identifying and evaluating risks, along with their likelihood and consequences, in order to enhance the risk assessment process there. To ensure that the risk assessment process is thorough and reflects the organization's assets, threats, and vulnerabilities, it is also critical to continuously review and update it. The risk assessment may also benefit from the participation of a wide range of stakeholders, as this can help guarantee that all potential risks are identified and taken into consideration.

1. **Benefits from the ISO Risk Management Methodology:** (ISO, 2018b, 2018a; Peterson, 2019; Posey, 2021)

ISO 31000 is a risk management standard that offers businesses with a framework for identifying, assessing, and managing risks. Moreover, it is intended to be adaptable and applicable to any organization, regardless of size or sector. The standard contains guidance for executing a risk management process, such as defining risk management strategies, identifying risks, assessing their likelihood and impact, and monitoring and analyzing the success of those methods.

Adopting an appropriate risk management approach, such as the ISO 31000 methodology, can provide a number of benefits for the IT security of this project.

1. Proactive threat detection and mitigation steps lower the risk of a security event occurring.
2. By identifying and assessing risks, the company can gain a better understanding of potential threats and weaknesses that could impair the business.
3. Prioritizing the most critical risks based on likelihood and impact, allowing the business to focus on the most critical risks and allocate resources accordingly.
4. The organization can reduce or eliminate the likelihood and impact of risks by implementing controls and mitigation measures. This can help the organization protect its vital assets and ensure the confidentiality, integrity, and availability of its systems and data.
5. By monitoring and analyzing the risk management process on a regular basis, the organization may stay current on the latest risks and vulnerabilities, as well as the effectiveness of the applied controls and mitigation measures. This can help the organization respond quickly to developments while also protecting itself from new threats.
6. Creating a consistent and systematic approach to risk management that ensures all risks are consistently identified and evaluated.
7. Providing a clear and objective risk assessment so that the organization may make educated risk management decisions.
8. Improving stakeholder communication and collaboration by developing a common language and framework for discussing and addressing risks.

By identifying critical assets and conducting a risk assessment to identify potential vulnerabilities and threats, ISO 31000 can be utilized to strengthen the IT security of this project. The organization can then prioritize these risks based on their likelihood and impact, and establish risk mitigation or prevention initiatives. In addition, the organization should design a strategy for monitoring and analyzing the efficacy of these tactics as the project progresses, and make any necessary changes.

Furthermore, the risk treatment procedure in the standard can assist the team in identifying and efficiently applying the most appropriate risk treatment solutions. This can help to reduce the probability and impact of recognized threats while also increasing overall project security.

Moreover, ISO 31000 emphasizes the importance of communication and consultation throughout the risk management process. This can help to ensure that all stakeholders are aware of the identified risks and mitigation strategies. It can also help to build support for the project's IT security measures and ensure their effective implementation.

In conclusion, the ISO 31000 risk management methodology can provide a systematic and comprehensive approach to managing risks in this project's IT security, assisting the project team in identifying, assessing, and treating IT security risks, prioritizing them based on their likelihood and potential impact, and implementing appropriate controls and mitigation strategies to address them in order to protect its critical assets and ensure the confidentiality, integrity, and availability.

1. **Misalignment of IT Security with Warmaksan Policy:**
2. **The Security Impact of this Misalignment:**

Misalignment of IT security with Warmaksan's security policy can have a number of severe consequences for the company's network resources, data, and information security.

For example, if the organization's policy restricts employees from using VPNs but the IT Security Policy allows the usage of encrypted VPNs while working remotely, this mismatch might cause employee confusion because they may be unaware of the proper protocols to follow when working remotely. Furthermore, this disparity may make it more difficult for Warmaksan to implement its security policy and ensure that all staff follows the same standards.

Moreover, this misalignment can lead to security flaws. For example, if an employee is ignorant that the usage of VPNs is restricted, they may use an unencrypted VPN, exposing the organization's data to threat actors. Allowing employees to use encrypted VPNs while working remotely may also lead to employees using VPNs that are not allowed by the organization’s policy, creating security concerns.

Furthermore, misalignment between the IT security policy and the overall security policy can also result in ineffective incident response and data recovery procedures. For example, if the IT security policy allows for data backup to occur in a cloud-based environment while the overall security policy prohibits the use of cloud storage, the organization may not have access to its data in case of a disaster or security breach. This can lead to significant financial losses and reputational damage for the company.

Finally, the misalignment of IT security with the overall security policy can also lead to non-compliance with legal and regulatory requirements, such as the GDPR. This can result in costly penalties, legal liabilities, and reputational damage for the organization.

In conclusion, misalignment of IT security with overall security policy can have serious consequences for Warmaksan, including security vulnerabilities, a lack of security controls, ineffective incident response and data recovery procedures, non-compliance with legal and regulatory requirements, and financial and reputational harm. Warmaksan must therefore integrate its IT security strategy with its overall security policy to ensure the safety of its network resources, data, and information security.

1. **Recommendations on How to Maintain their Alignment:**

To maintain alignment of IT security with Warmaksan's policy, the following recommendations can be implemented:

* + 1. **Establish a clear and comprehensive IT security policy:** The organization should create a clear and comprehensive IT security policy that specifies the firm's IT security objectives, goals, and expectations. This policy should be consistent with the organization's overall policy and should be reviewed and updated on a regular basis to ensure that it stays current, relevant, and consistent with the company's policy. It can also help to ensure that the policy is up to date with the current risks and vulnerabilities and remains consistent with the organization's broader policy and strategy.
    2. **Involve all stakeholders in the development and review of the IT security policy:** To ensure that the IT security policy is consistent with the organization's overall policy and strategy, it is critical to include all stakeholders in the policy's development and revision. This can help to ensure that the policy reflects the needs and concerns of all stakeholders, increasing the likelihood that it will be supported and executed, and ensuring that is in line with the overall policy.
    3. **Conduct regular security audits and assessments:** Conducting security audits and assessments on a regular basis can assist the company in identifying any misalignment between IT security and Warmaksan's policy. By identifying any gaps, misalignments, or inconsistencies in the firm's security posture, the organization may take steps to fix them and assure overall policy and plan alignment.
    4. **Ensure compliance with industry standards and regulations:** Warmaksan must comply with a variety of IT security regulations and standards, such as the GDPR and PCI DSS. It is critical to ensure that the IT security policy and Warmaksan's overall policy are both aligned with each other and with these regulations and standards to minimize the risk of non-compliance and penalties.

1. **Warmaksan’s Security Policy:** Warmaksan’s security policy is included in the appendix of this document.
2. **Justification of the Developed Security Plan:**

The following is a justification of the developed security plan, by providing reasons for the elements that were selected. This involves explaining the reasoning behind the decisions made regarding the specific security measures included in the plan, and how they address potential security risks.

* + 1. **Warmaksan Network Security Policy:** This policy's components were chosen to maintain the confidentiality, integrity, and availability of the company's network resources and data. Restricting network access to authorized users only and requiring valid usernames and passwords aids in preventing unauthorized network access. Installing and configuring current antivirus software on all network-connected devices aids in the prevention of malware and other cyber risks. Monitoring network traffic for security breaches and unusual activities assists in promptly detecting and responding to potential security events. Prohibiting users from installing software or making modifications to network-connected devices without the consent of the IT department helps to guarantee that devices are properly configured and maintained, while also ensuring that any software installed is valid and not malicious. Prohibiting the use of business resources for personal benefit or activities that may harm the company's reputation or financial well-being helps to maintain the organization's reputation and the trust of clients, partners, and stakeholders.
    2. **Warmaksan Password Policy:** This policy's components have been chosen to safeguard the confidentiality and integrity of the company's systems and data, as well as the privacy of its employees and customers. Requiring strong, complicated passwords that are at least 8 characters long and contain a mix of letters, numbers, and special characters helps to defend against password guessing or cracking. Passwords should be changed at least every 90 days to prevent against unauthorized access if a password is compromised. Prohibiting the inclusion of personal information or easily guessable words in passwords helps to defend against hostile actors guessing or acquiring personal information. Passwords should not be written down or discussed, and users should update their passwords and tell IT if they suspect a compromise. This helps to ensure that passwords are kept secure.
    3. **Warmaksan Data Loss Prevention Policy:** This policy's components were chosen to prevent the loss of sensitive or secret information. It provides rules for data backup, encryption, retention, and destruction, and it aids in the prevention of data breaches, leaks, theft, and corruption.
    4. **Warmaksan Disaster Recovery Plan:** This plan's components were chosen to assure the continuance of the company's business operations in the case of a disaster. It comprises standards for data backup, data replication, data recovery, and disaster recovery testing, and it aids in ensuring that the company's data and systems are available in the case of a disaster, as well as minimizing the impact of a disaster on the company's business activities.
    5. **Warmaksan Data Retention Policy:** The policy features were chosen to ensure that the company's data is correctly preserved for legal and regulatory compliance, as well as for business interests. It comprises standards for data archiving, deletion, and retention periods, and it assists in ensuring that the organization's data is appropriately retained and disposed of in accordance with legal and regulatory obligations as well as company policies.
    6. **Warmaksan Access Authorization, Modification, Identity Access Management, Access Control, and Authentication Policy:** The elements of this policy have been chosen to ensure that only authorized individuals have access to the company's data and systems, and that access is properly regulated, managed, and audited. It comprises standards for user authentication, access control, logging, and revocation, and it aids in ensuring that only authorized personnel have access to the company's data and systems, and that access is appropriately regulated, managed, and audited.

1. **Evaluation of the Suitability of the Tools Used in the Policy:**

The Warmaksan Security Policy uses a variety of tools to ensure the security of its systems and networks.

1. **Firewall:** This is a detective and preventive tool that helps to block unauthorized access to the network by controlling the flow of incoming and outgoing traffic. It acts as a barrier between the internal network and the external network and can be configured to allow or block specific types of traffic based on predefined rules.
2. **Intrusion detection and prevention system (IDPS):** This is a detective, preventive and corrective tool that monitors network traffic for suspicious activity and alerts security personnel of any potential security breaches. It can also prevent known attacks by blocking traffic that matches a predefined set of rules.
3. **Antivirus software:** This is a preventive tool that scans for and removes malware from the system. It can also prevent new infections by blocking known malware from being downloaded or executed.
4. **Strong passwords:** This is a preventive and deterrent tool that helps to prevent unauthorized access to the system by requiring users to use strong, complex passwords that are difficult to guess or crack.
5. **Network segmentation:** This is a preventive tool that helps to limit the spread of malware or other malicious activity by isolating different parts of the network from each other. This makes it harder for an attacker to move laterally within the network and compromise other systems.
6. **Regular backups:** This is a recovery tool that helps to ensure that data can be restored in the event of a disaster or data loss. Regular backups of important data can help to minimize the impact of a security incident.
7. **Regular security audits and penetration testing:** This is a detective, corrective and compensating tool that helps to identify and fix vulnerabilities in the system. Security audits are used to identify and assess vulnerabilities, while penetration testing is used to test the effectiveness of the security controls in place.

The Warmaksan Security Policy uses a combination of deterrent, directive, preventive, detective, corrective, compensating, and recovery tools to ensure the security of its systems and networks.

1. **The Roles of Stakeholders in Implementing Security Audit Recommendations:**The implementation of security audit recommendations is a collaborative effort that involves a wide range of stakeholders within the Warmaksan organization. Each stakeholder plays a specific role in ensuring that the recommendations are implemented effectively and efficiently.
2. **The IT department:** The IT department is crucial in putting security audit recommendations into action. They are in charge of configuring and maintaining the security audit's suggested technological measures, such as firewalls, intrusion detection systems, and antivirus software. They are also crucial in monitoring the network for security breaches and unusual activities, as well as responding to any incidents that are discovered.
3. **The management team:** The management team is responsible for providing the resources and support needed to put security audit recommendations into action. This includes financing for new security procedures as well as ensuring that the required staff and equipment are on hand to put the recommendations into action. The management team is also responsible for explaining the importance of security to the rest of the business and ensuring that all employees are aware of their security duties.
4. **The employees:** Employees are crucial in ensuring that security audit recommendations are appropriately implemented. They are accountable for adhering to security standards and procedures, as well as reporting any suspicious activity or security breaches. Employees also play an important part in ensuring the confidentiality and integrity of the company's data and systems by adhering to best practices in password management and information security.
5. **External Auditors:** External auditors are responsible for providing an objective assessment of the organization's security posture, identifying areas of vulnerability, and recommending adjustments. They are also in charge of overseeing the implementation of the recommendations to ensure that they are adequate and effective.
6. **Compliance team:** since Warmaksan is obliged to meet industry-specific compliance standards, such as GDPR, the compliance team will be responsible for ensuring that the security audit recommendations meet these requirements.
7. **Legal team:** To ensure that the organization complies with all relevant laws and regulations, the legal team may be involved in implementing security audit recommendations relating to data privacy and security.
8. **Risk management team:** The risk management team is responsible for identifying, assessing, and prioritizing threats to the company, as well as evaluating security audit recommendations in relation to the risk profile.

To ensure that security audit recommendations are effective, it is critical that all stakeholders understand their roles and responsibilities and are completely committed to implementing them. Regular communication and updates are required to keep everyone informed and engaged in the process, as well as to guarantee that the suggestions are being implemented as planned. By incorporating all key stakeholders in the implementation of security audit recommendations, the organization can guarantee that the recommendations are aligned with the goals and requirements of the entire organization and that they will be implemented and maintained effectively over time.

# ***References***

Buckbee, M. (2020) What is an IT Security Audit? The Basics, Varonis. Available at: <https://www.varonis.com/blog/security-audit>

CCOHS (2021) Hazard and Risk - Risk Assessment : OSH Answers, CCOHS. Available at: <https://www.ccohs.ca/oshanswers/hsprograms/risk_assessment.html>

ISO (2018a) ISO - ISO 31000 — Risk management, ISO. Available at: <https://www.iso.org/iso-31000-risk-management.html>

ISO (2018b) ISO 31000:2018(en), Risk management — Guidelines, ISO. Available at: [https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en](https://www.iso.org/obp/ui/%23iso:std:iso:31000:ed-2:v1:en)

Lucidchart (2020) A Complete Guide to the Risk Assessment Process, Lucidchart. Available at: <https://www.lucidchart.com/blog/risk-assessment-process>

Peterson, O. (2019) What Is ISO 31000? Getting Started with Risk Management | Process Street | Checklist, Workflow and SOP Software, Process.St. Available at: <https://www.process.st/iso-31000/>

Posey, B. (2021) What is the ISO 31000 Risk Management Standard?, Online Article. Available at: <https://www.techtarget.com/searchsecurity/definition/ISO-31000-Risk-Management>

Satori (2022) Data Protection and Privacy: 12 Ways to Protect User Data, Cloudian. Available at: <https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/>

SNIA (2020) What is Data Protection?, SNIA. Available at: <https://www.snia.org/education/what-is-data-protection>

StandardFusion (2022) What is an IT Security Audit?, StandardFusion. Available at: <https://www.standardfusion.com/blog/what-is-an-it-security-audit/>

Tajuddin, A. (2021) Risk Assessment Procedures - step to prepare risk assessment, Safety Notes. Available at: <https://www.safetynotes.net/risk-assessment/>

Varghese, J. (2021) IT Security Audit: Importance, Types, and Methodology, Astra. Available at: <https://www.getastra.com/blog/security-audit/it-security-audit/>

# ***Security Policy***

Warmaksan is dedicated to ensuring the safety of its data, systems, and networks. Warmaksan created this security policy to safeguard the confidentiality, integrity, and availability of these resources. This policy describes the guidelines and procedures for the secure use of Warmaksan's network resources. It is intended for all individuals and devices that use or connect to Warmaksan's network, and it will be regularly audited to ensure its implementation throughout the company. We can work together to protect Warmaksan's precious assets and keep the trust of our clients, partners, and stakeholders by adhering to this policy.

Failure to adhere to this policy may result in disciplinary action, including termination of employment or contract. Noncompliance with this policy may also have legal and financial ramifications for both the individual and the firm. All individuals covered by this policy are responsible for becoming acquainted with its contents and adhering to its obligations.

1. **Warmaksan Network Security Policy:**

**Purpose:**

The purpose of this policy is to create standards for the safe use of Warmaksan's network resources, such as computers, servers, and other connected devices. Its purpose is to safeguard the confidentiality, integrity, and availability of these resources, as well as the data and information they contain.

**Scope:**

This policy applies to all users and devices that utilize or connect to Warmaksan's network. It applies to all network-connected devices, including desktops, laptops, servers, routers, switches, and other hardware and software.

**Policy:**

1. Only authorized users have access to Warmaksan's network. To access the network, users must have a valid login and password.
2. All network-connected devices must be equipped with up-to-date antivirus software and set up to receive automatic updates.
3. Users must not install software or make changes to network-connected devices without the IT department's consent.
4. Users are not permitted to utilize Warmaksan's network resources for personal benefit or to engage in activities that may harm the company's reputation or financial well- being.
5. Users must keep sensitive or proprietary information confidential. This includes safeguarding such information against illegal access, use, or disclosure.
6. Warmaksan's network must be accessed remotely via a secure, encrypted connection using a Virtual Private Network (VPN).
7. Only authorized people should have physical access to network-connected equipment. When not in use, all devices must be properly locked.
8. Warmaksan’s network must be protected using a variety of physical and virtual security measures such as implementing an IDPS, firewalls, encryption, security cameras, locks, etc.
9. Warmaksan’s network must be segmented into a number of subnets, including a DMZ.
10. **Warmaksan’s Password Policy:**

**Purpose:**

The goal of this policy is to provide rules for password security inside Warmaksan. It is meant to protect Warmaksan's systems and data, as well as the privacy of its employees and customers.

**Scope:**

This policy applies to all anyone who use passwords to access Warmaksan's systems. It is applicable to all password-protected systems, such as computers, servers, and other devices.

**Policy:**

1. All passwords must be kept secure and must not be shared with others.
2. Passwords must be at least 8 characters in length and must include a combination of letters, numbers, and special characters.
3. Passwords must be changed once every 90 days.
4. Passwords must not be based on personal information or easily guessable words.
5. If a user suspects that their password has been compromised, they must immediately change their password and notify the IT department.
6. In the event that a password is lost or forgotten, the user must contact the IT department for assistance in resetting their password.
7. **Warmaksan Data Loss Prevention Policy:**

**Purpose:**

This policy is intended to set rules for the secure management of sensitive and proprietary data inside Warmaksan. It is designed to protect against unauthorized access, use, or disclosure of this data, as well as data loss, corruption, or destruction.

**Scope:**

This policy applies to all individuals and devices within Warmaksan who handle or access sensitive or proprietary data. It addresses all modalities of data storage and transmission, including physical documents, computer files, and email.

**Policy:**

1. Only authorized users have access to sensitive or proprietary data. To access data systems, users must have a valid username and password and must adhere to all established access rules and protocols.
2. To prevent unwanted access, all data storage and communication protocols must be encrypted.
3. Data must be backed up on a regular basis to ensure its recovery in the case of loss or corruption.
4. Users shall not disclose sensitive or confidential information to unauthorized individuals or organizations.
5. Users must keep sensitive or proprietary data confidential. This includes safeguarding such data against illegal access, use, or disclosure.
6. Warmaksan's data systems must be accessed remotely via a secure, encrypted connection via a Virtual Private Network (VPN).
7. Only authorized individuals should have physical access to data storage devices. When not in use, all devices must be properly locked.
8. **Warmaksan Disaster Recovery Plan:**

**Purpose:**

The purpose of the plan is to create guidelines for responding to and recovering from disasters that may impact Warmaksan's network resources, such as computers, servers, and other connected devices. Its goal is to reduce downtime while also ensuring the security, integrity, and availability of these resources, as well as the data and information stored on them.

**Scope:**

This policy applies to all people and devices who use or connect to Warmaksan's network. It includes desktops, laptops, servers, routers, switches, and other network-connected hardware and software.

**Plan:**

In the event of a disaster that affects Warmaksan's network or network-connected devices, the following steps will be taken:

1. The IT department will determine the degree of the damage and the cause of the incident.
2. The restoration of important systems and services will be prioritized by the IT department.
3. If necessary, emergency backup systems will be triggered to ensure the continued availability of critical services.
4. The IT department will work as rapidly as possible to restore all affected systems and services.
5. The IT department will examine the disaster recovery plan and make any required changes to better prepare the organization for future calamities.

Failure to adhere to this plan may result in extended downtime and the loss of critical data and information. All individuals covered by this plan are responsible for becoming acquainted with its contents and following the measures provided in the event of a disaster.

1. **Warmaksan Data Retention Policy:**

**Purpose:**

The goal of this policy is to set rules for proper data handling, storage, and destruction at Warmaksan. Its purpose is to safeguard the security, integrity, and availability of this data while also ensuring compliance with legal and regulatory obligations such as the GDPR.

**Scope:**

This policy applies to all individuals and devices at Warmaksan who handle, store, or transfer data. It encompasses all data types, including electronic and physical records, as well as any devices and systems used to access or process this data.

**Policy:**

1. Data must be handled, stored, and communicated in such a way that its confidentiality, integrity, and availability are protected.
2. Data access must be restricted to just authorized individuals. To access data, users must have a valid username and password.
3. When data is transported across a network or kept on portable devices, it must be encrypted.
4. Data must be backed up on a regular basis to enable its recovery in the case of a disaster or data loss.
5. Data retention schedules must be followed to ensure that data is retained for the required period of time and then disposed of correctly when no longer required.
6. Data must be disposed of securely, for as by using data destruction software or physically destroying media.
7. Any suspected data breaches or unauthorized data access must be immediately notified to the IT department.
8. **Warmaksan Access Authorization, Modification, Identity Access Management, Access Control, and Authentication Policy:**

**Purpose:**

The purpose of this policy is to ensure that only authorized users have access to Warmaksan's resources, as well as to regulate and monitor that access and modification. Its purpose is to safeguard the confidentiality, integrity, and availability of these resources, as well as the data and information they contain.

**Scope:**

This policy applies to anybody who uses or connects to the Warmaksan network. It includes desktops, laptops, servers, routers, switches, and other network-connected hardware and software.

**Policy:**

1. To access Warmaksan's resources, users must utilize their own unique login credentials. Sharing login information is strictly banned.
2. Resource access is assessed on a regular basis and may be discontinued at any time if an individual's job or responsibilities change.
3. All resource access and modification must be reported and monitored. Any suspicious behavior or illegal access must be immediately reported to the IT department.
4. Users are not permitted to utilize Warmaksan's resources for personal benefit or to engage in activities that may harm the company's reputation or financial well-being.
5. The IT department is in charge of managing and maintaining all access control lists and permissions.
6. To protect the security of access to Warmaksan's resources, authentication mechanisms such as passwords and two-factor authentication must be examined and updated on a regular basis.
7. In the case of a security breach, the IT department will undertake an extensive investigation and take the necessary steps to secure the impacted resources and prevent future breaches.

# ***Student Declaration Form***