Information Security Management System

Jonathan Park

Security Frontline

for client:

Shameless Insurance Ltd

Version Control

Date	Author	Version	Description
7 Sept 2023	Edhita Singhal, Jonathan Park & Sonya de Urioste	01	The obligations and scope for Shameless Insurance
14 Sept 2023	Edhita Singhal, Jonathan Park & Sonya de Urioste	02	BIA
29 Sept 2023	Edhita Singhal, Jonathan Park & Sonya de Urioste	03	Asset Management System
27 Oct 2023	Edhita Singhal, Jonathan Park & Sonya de Urioste	04	Risk Management
17 Nov 2023	Brad Williams, Constantine Trubitski & Jonathan Park	05	Incident Response
12 Dec 2023	Jonathan Park	06	Policies and Controls

Table of Contents

Separately attached:

Asset Register

Risk Register

Gantt Chart

Executive summary

Overview

Security Frontline has been called by client Shameless Insurance Ltd. to audit the company and produce an information security management system. This resulting ISMS provides Shameless a structured information security program spanning asset and associated risk management, incident response and recovery, and recommended policies governing employee cybersecurity postures — which, if successfully implemented, will altogether demonstrate a newfound commitment by Shameless to being fully up to standard and beyond in its cybersecurity profile, and thus rebuild trust with the customer base. — *see sections 1.2, 1.3, 1.4*

Scope

This resulting comprehensive document will focus on the head office in Bridlington, with the other offices in Los Angeles and New Delhi not considered. All business elements within all departments of the Bridlington office are subject to this audit. This project has a budget of $600,000; completion is projected to take 12 months. — *See section 2*

Greatest risks and recommendations

- **Outdated software**: Patch software to the latest versions wherever possible. Prioritize Shameless's web servers, which are severely outdated. — *See attached risk register*
- **CEO behavior and leadership**: The CEO sets the tone and culture from the top-down. CEO must cooperate with managerial staff and IT department and offer support wherever budget and time allow in order to instill a proper culture around cybersecurity.
- **Lack of security policies**: Implement a comprehensive set of policies governing company data, security, employee access, etc., not least of which should be the four policies in section 6.3 of this ISMS. — *see section 6*
- **Lacking staff culture around cybersecurity**: Incorporate and require trainings on user awareness, as well as trainings to educate employees about the company's new security policies once they are implemented. — *see section 4.3*
- **Lacking processes to record and track assets**: Build upon Security Frontline's provided asset management workflow, or alternatively, invest in proprietary asset management software. — *see section 3.6*

Legal requirements

Shameless is subject to the European Union's General Data Protection Regulation (GDPR) law; the United Kingdom equivalent (UK GDPR); the California Consumer Privacy Act (CCPA); India's Digital Personal Data Protection Act; and the Payment Card Industry Data Security Standard (PCI DSS). Violations of these laws can easily overlap and result in millions of pounds in fines, sometimes calculated as a portion of the company's profits. Compliance with these laws requires demonstrable systems that strongly protect and restrict customer data; CCPA especially requires that consumers can request and delete all of their personal data from the company's servers. — *see section 1.6*

1 — Introduction and Obligations

1.1 Introduction to Security Frontline

Thank you for choosing Security Frontline to implement changes to the cybersecurity protocols of Shameless Insurance. We have aimed to create an Information Security Management System for Shameless, outlining the steps that we believe should be taken in the next 12 months to improve the company's cybersecurity posture. We would like to thank the CEO, Head of IT, and Network Manager for their contributions to the ISMS, and for providing us with the necessary information to build it.

1.2 Introduction to ISMS

It is our understanding that at Shameless Insurance Ltd., information and data are synonymous with the business; without well-protected information, there is no business. So it follows that protecting this company's information is of utmost priority. To accomplish this in any capacity, having an information security management system (ISMS) is the bare minimum. An ISMS is a collection of software, hardware and, perhaps most importantly, policies, with the primary goal of defending the networks and servers that comprise the company, and the data contained therein. It encompasses a set of guidelines and protocols intended to carefully oversee an organization's confidential information.

Typically, an ISMS addresses employee behavior, operational procedures, and data and technological aspects. ISMS has the ability to be customized to specific data categories, such as customer information, or it can be integrated comprehensively into the company's culture.

1.3 Purpose of an ISMS

The leading ambition of implementing an ISMS is to demote potential risks and ensure the uninterrupted operation of the business by actively mitigating the consequences of any security breaches. It protects the confidentiality, integrity and availability of the organization's data through a cohesive set of requirements that can be followed at the time of breaches and cyber attacks, making sure there is a course of action.

It is extremely useful for businesses that want to safeguard their organizations from cyber threats, uphold their reputation, and avoid potential fines resulting from security breaches or policy violations, such as GDPR or CCPA non-compliance. These measures not only benefit the company by protecting its interests but also extend benefits to clients and employees who can trust the security of their data. ISMS not only safeguards the business but also fosters trust and security for both clients and staff alike.

1.4 Benefits of ISMS

The ISMS gives a comprehensive method for overseeing the information systems within an organization. It reduces the likelihood of breaches, and damage done by breaches, restores reputation and/or trust with customers, potentially attracts new customers, and overall benefits the usability of the network in general for employees' day-to-day.

By introducing an ISMS now, Shameless can work towards restoring its reputation and clients' trust that it previously lost. Furthermore, since it has offices in the UK, Los Angeles and India, Shameless must be UK GDPR, CCPA, and Digital Personal Data Protection Act compliant or incur high fines, which would only further reduce its revenue. Through the ISMS, this can be combated, hence benefiting the company. Lastly, an ISMS will also yield benefits for other stakeholders, such as clients and employees, whose personal data will be protected and not leaked on public forums.

1.5 ISMS Protection Capabilities

ISMS will assist Shameless in combating and protecting against breaches, unauthorized access, and bugs. As well as data leaks on public forums such as Reddit, hardware/software failure, and application layer attacks that are continuously breaching the organization's ineffective firewalls. It will also set clear policies for employee training, ensuring that they don't fall prey to phishing emails or change their passwords to prevent hacks.

1.6 Legal Requirements and Potential Fines

Shameless Insurance, Ltd. is subject to several data protection and cybersecurity regulations that carry substantial penalties for noncompliance. Failure to comply with these laws can result in severe fines and reputational damage.

1.6.1 General Data Protection Regulation (GDPR)/UK GDPR

- The GDPR allows for fines of up to £20 million or 4% of Shameless' total worldwide annual revenue from the previous financial year, whichever is higher, for violations.
- Lack of vulnerability patching that leads to a data breach could be considered negligence under the GDPR and carries significant fines. Shameless must maintain reasonable security practices.
- The GDPR requires timely restoration of personal data availability after an incident. Shameless' recent hardware failure and data loss due to poor backup systems violates this requirement.
- Failing to encrypt sensitive client data also violates GDPR and can incur fines.

1.6.2 California Consumer Privacy Act (CCPA)

- The CCPA allows for fines of $7,500 per intentional violation or $2,500 per unintentional violation.

- Not providing customers proper notice of data collection practices or the ability to delete data could lead to fines under the CCPA.
- The recent data breach of 1,000 client records due to a patch failure is considered non-intentional and carries an estimated $2,500 per record fine.

1.6.3 Digital Personal Data Protection Act (India)

- Violations can lead to fines up to 250 crore rupees ($30 million USD).

1.6.4 Payment Card Industry Data Security Standard (PCI DSS)

- Selling cyber insurance and internet-connected security cameras requires PCI DSS compliance.
- Noncompliance fines can range from thousands to hundreds of thousands of dollars.

Shameless must take data protection and cybersecurity legal requirements seriously. Failure to comply with the above laws and standards can lead to substantial financial penalties and reputational damage. We must review and enhance our policies, systems, and processes regularly to avoid violations.

2 — Scope

2.1.1: Scope

This ISMS will focus on the head office of Shameless Insurance, Ltd located in Bridlington, U.K. The review will encompass the IT, HR and Finance Departments which are located at this Head Office location.

The timeframe for this review will be the next 12 months, beginning as soon as approval is obtained. The budget allocated for this project is $600,000.

This review is strictly limited to the Bridlington office, and does not include Shameless' satellite offices in Los Angeles and New Delhi. Those locations are outside the scope of this specific project.

Remediation and enhancement of cybersecurity and compliance for the Los Angeles and New Delhi satellite offices will need to be covered in separate future projects with their own scope and budgets.

2.1.1: Activities and Processes

The goal of this 12-month review is to thoroughly analyze and audit our cybersecurity and data protection policies, procedures, and systems at the Bridlington office. We will identify any gaps or areas of non-compliance with regulations like the GDPR, CCPA, and PCI DSS. The review will generate actionable recommendations for enhancing the Bridlington office's cybersecurity and compliance posture within the allocated budget.

Through this ISMS, Shameless should have the ability to detect and protect its data against future cyber attacks. For example, to avoid phishing attacks and data leaks, policies for employee training and periodic password changes will be introduced. More coherent processes with uniform documentation will be put in place, which Shameless can refer to while addressing breaches and threats, increasing their reaction speed and ability to protect all assets.

Through such steps, we will elevate Shameless from Tier 1 of the NIST cybersecurity framework maturity level to Tier 2, where they are risk-informed. The frameworks and processes will initially only be implemented in the Bridlington office and not organization-wide.

With the enforcement of this ISMS, Shameless will stop violating regulations, such as the GDPR, and won’t be fined under them anymore, in turn, helping their revenue.

2.2: Scope Justification

The ISMS will be focusing on the Head Office, situated in Bridlington UK because this is where a majority of the employees are located, including the IT department. We will be focusing on all departments located in the Head Office, such as IT, Finance and HR departments. These departments deal with sensitive client and employee data so we will ensure that their systems are safe and GDPR compliant.

According to a survey conducted by Deloitte (Bernard et al., 2020), finance companies spend an average of 10.9% of their IT budget on cybersecurity, or 0.48% of their total revenue. Hence, applying these industry standards to Shameless' last year's revenue of $50 million, they should spend $240,000. However, since Shameless has had minimum spending on cybersecurity in the last decade and lacks updated systems and trained employees who can fix this, a drastic change in the organization's cybersecurity operations is needed. Hence, a budget of $750,000, which is 1.5% of the entire revenue is needed to create a meaningful change in the organization.

Currently, we aren't including all departments because of budgetary constraints. However, we will introduce these new policies and changes in the Head Office for 12 months and after testing them and evaluating results and areas of improvement, we will push the changes to the satellite offices in Los Angeles and New Delhi.

3 — Asset Management

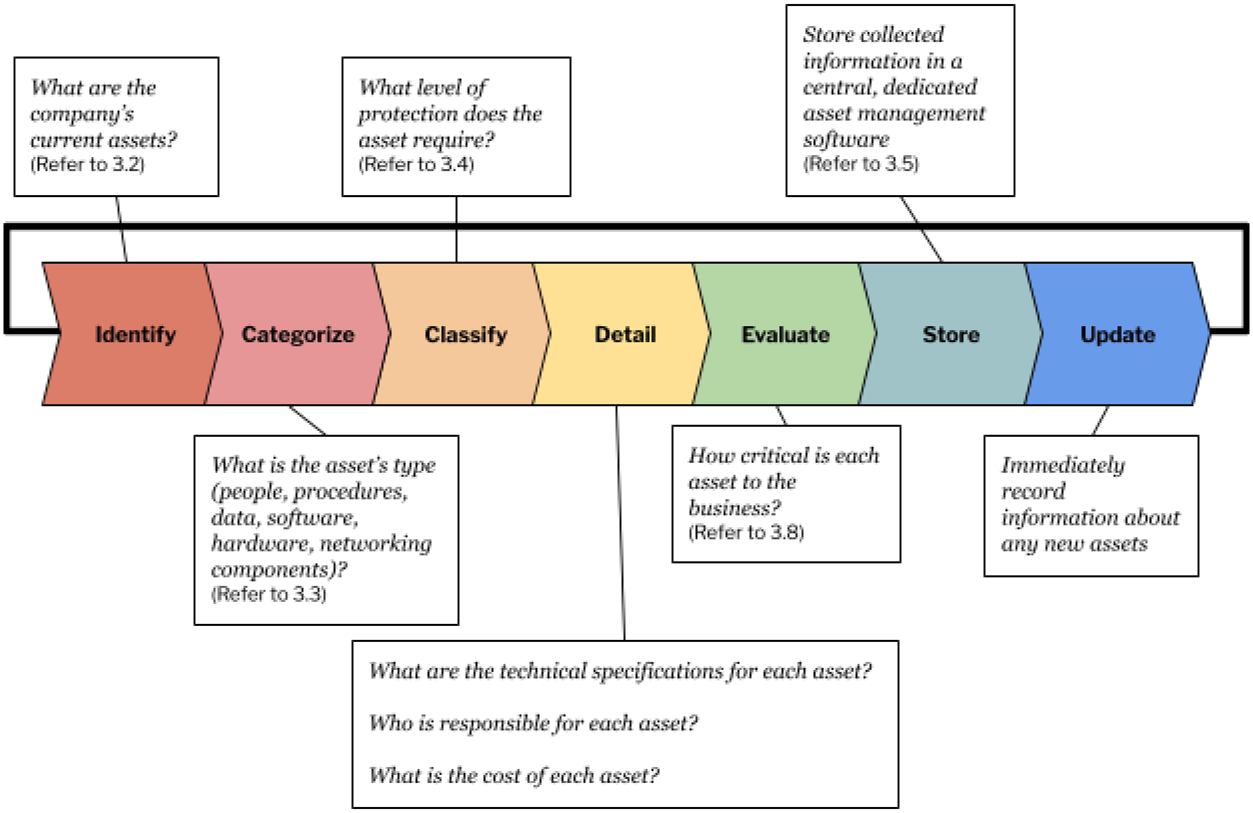

What are the company's current assets? (Refer to 3.2)
What level of protection does the asset require? (Refer to 3.4)
Store collected information in a central, dedicated asset management software (Refer to 3.5)
Identify
Categorize
Classify
Detail
Evaluate
Store
Update
What is the asset's type (people, procedures, data, software, hardware, networking components)? (Refer to 3.3)
How critical is each asset to the business? (Refer to 3.8)
Immediately record information about any new assets
What are the technical specifications for each asset?
Who is responsible for each asset?
What is the cost of each asset?

Figure 3.1: A flow chart visualizing the asset management process.
For specifics about the information and specifications required for each asset, please refer to the attached Asset Register.

3.1 Assets and Asset Management

According to NIST SP 800-160v1r1 (Ross et al., 2022), an asset is anything of value to the business and can be of various types, including tangible and intangible. Asset management is an up-to-date register with all of the company's tangible and intangible assets so the organization has an organized and coherent list available for future use. NIST recommends that an organization have an asset register, but it doesn't provide specific details. Hence, we have used the framework to customize one for Shameless.

By recording all the available assets, their valuation over time, and when they need to be updated or replaced, the company is able to maximize the use of each asset and save money. Moreover, this will allow for more efficient planning in case systems are lost or need to be changed and it also makes employees more accountable since they are aware of their responsibilities.

3.2: Process of Asset Identification

The first step is identifying all information assets owned by the company and creating an inventory of them. Here, all assets, from employee work phones to databases, staff and policies must be identified and recorded.

3.3: Categorization

The second step is categorizing assets into different system components. While NIST provides numerous asset types (Ross et al., 2022), we recommend the following 6 for Shameless: People, Procedures, Data, Software, Hardware and Network Components (refer to Asset registry spreadsheet attached and the table below for which assets fall under which category).

The Asset Register attached includes some of the assets in the Bridlington office with various columns that hold necessary information about each asset. This procedure should be continued when new assets are added and for the Los Angeles and New Delhi offices.

It's important to categorize assets because each asset type has specific details that need to be recorded in the register and these details vary for each asset type and may not be applicable for all. For example, while each Hardware has a MAC Address, this information is not applicable to the employees of the company. In turn, while this information is recorded under the Hardware category, it won't be recorded under the People category.

Hence, instead of leaving empty columns, it's better to categorize and organize all the assets based on their type. This is more efficient to maintain and it will be easier to find/add assets and their relevant information in the future.

Asset Type	**Description**	**Example**
Hardware	Physical components and devices owned by the company.	Laptop, Database
Software	The program, operating system and other operating information used by the company	MOVEit Cloud
Network Components	Networking components are the devices and hardware utilized to create and sustain a computer network. It is also extremely important for an	Routers, VPN, Firewall

	organization to determine if a device is mainly a computer or mainly a networking device.	
People	Employees and staff of the company	CEO, Network Manager
Policy and Procedures	These are the documents developed for appropriate conduct at the workplace	Password Policy, Encryption Policy
Data	This includes all the information collected about clients, employees, vendors and other third parties	Client address, Employee Bank Account number

3.4 Appropriate Classification Scheme

NIST recommends developing and utilizing an Appropriate Classification Scheme based on the sensitivity and security required for the data. This needs to have extremely specific categories so that employees know the correct procedure to handle the data based on their level of protection. While the data can be categorized as High, Medium, and Low sensitivity, these are generic terms. Hence, it's recommended that Shameless uses a more detailed classification approach so it's easier for employees to identify the data and take correct precautions.

There are 5 levels of classification for assets:

Public Data: This is the lowest level of protection. Public and non-employees also have access to this information and it doesn't need protection. An example of this, would be the company mission statement or employee names.

Private Data: This data comes second and is protected from public view and unauthorized access because it can harm the organization. A key example of this would be passwords to employee emails or office-related accounts.

Confidential Data: Third, there is confidential data which if leaked would cause more harm to the company than the leak of private data. For example, customer data, such as bank accounts or future plans will damage the company's reputation and may potentially lead to a loss of clients and, in turn, a loss of revenue.

Proprietary Data: This data is specific to the company and isn't often disclosed to third parties because if leaked, it can reduce the company's competitive advantage. An example of this is intellectual property and product costing.

Critical Data: This can cause the most amount of damage to the company. This includes details about new products or trade secrets, which can cause a huge loss in revenue and reputation.

3.5 Identification and Storage

Identifying, storing, and keeping track of assets within an organization is a critical component of asset management. The specific type of information to track depends on several factors such as the specific needs of the organization and its risk management efforts.

It's important that the asset register is extremely accessible and it is easy to find the needed asset and its information. This is done by categorizing the assets into asset types (check 3.3 of the ISMS) and the spreadsheet attached has a separate sheet for each asset type. This categorization also offers the employee some flexibility while adding a new asset because each category has its own specific columns, such as Asset ID, Asset owner, MAC Address, which may not be relevant to the other asset types. While adding a new asset, ensure that all the columns are filled out correctly and you don't leave even a single one blank because this is important data that will be useful in the future.

We strongly advise that whenever a new asset is acquired, you first input it into the spreadsheet with all the relevant information before passing it on to its owner. For example, if the Head of IT is receiving a new laptop, first add the laptop to the Hardware category and input all the relevant information, such as the asset tag, model, manufacturer and asset owner before passing on the new laptop to the employee. Putting this practice in place will ensure that all the assets are documented.

For now, while we advise that you use spreadsheets, in the future, we highly recommend using a type of asset management software such as Asset Panda (check 3.6 of the ISMS).

3.6 Software and Processes

3.6.1 Process Steps

It is extremely important for Shameless to consistently have their assets under control and managed. Currently, we have compiled a spreadsheet for the asset register.

There is a process one follows to add an asset to the register, which was carefully created to incorporate all asset information needed for the company. For example, the procedures tab in the spreadsheet is carefully organized into multiple columns to integrate all of the information needed regarding Shameless' policies and procedures. Here is an example of adding a Password Policy to the asset register (refer to 3.6.2 for the example image).

Step 1: Enter the PID number and procedure name, so one can use both to easily identify the procedure.

Step 2: Add a brief description outlining the contents or rules imposed by the policy document.

Step 3: Have a clear purpose that outlines the importance of having the procedure and the reason behind implementing it.

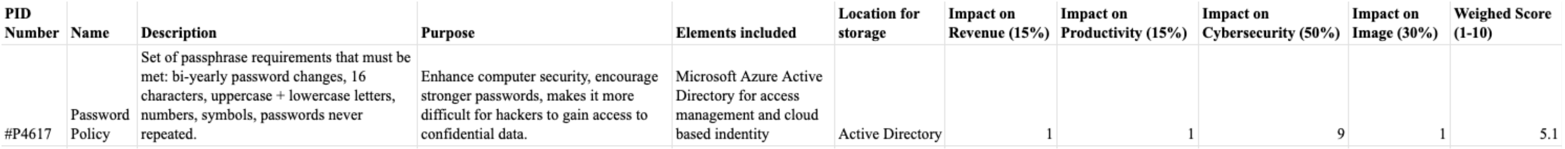
Step 4: In the elements included column fill out which devices/hardware/ software will be utilized to implement this procedure.

Step 5: The location of storage signifies “where to find the asset”.

Step 5: Then, logging the location of storage, which signifies “where to find the asset”, is crucial for efficient asset management, and aiding risk mitigation by offering valuable information for emergency preparedness and security measures.

Step 7: Lastly, you would rate the procedure in impact on a scale from 1-10 for revenue, productivity, cybersecurity, and image. Each impact criterion is weighted and differently impacts the final score. Refer to section 3.8 for the explanation and method on how to calculate this score.

3.6.2 Example



PID Number	Name	Description	Purpose	Elements included	Location for storage	Impact on Revenue (15%)	Impact on Productivity (15%)	Impact on Cybersecurity (50%)	Impact on Image (30%)	Weighed Score (1-10)
#P4617	Password Policy	Set of passphrase requirements that must be met: bi-yearly password changes, 16 characters, uppercase + lowercase letters, numbers, symbols, passwords never repeated.	Enhance computer security, encourage stronger passwords, makes it more difficult for hackers to gain access to confidential data.	Microsoft Azure Active Directory for access management and cloud based indentity	Active Directory	1	1	9	1	5.1

3.6.3 Alternate Softwares

While the spreadsheet is a good first step, as Shameless develops and acquires more assets, we suggest using other professional software, which will be easier to manage. Every company's assets are unique to their organization, so it's important to have software that is extremely quick and easy to customize, or add/remove users to enable them to have different levels of access. There are a few asset management software that we recommend:

1. Asset Panda: With asset management software such as Asset Panda (*About Asset Panda*, n.d.), Shameless will limit the risk of losing track of an item or tool, as well as where they are located and who is using them to deter loss and theft. Additionally, software like Asset Panda allows the company to easily perform routine maintenance and audits. These can be completed through a number of different methods: produce automated reports, schedule service and maintenance requests, as well as a new

built-in barcode scanner that quickly enables employees to easily locate the asset they are looking for.

2. ManageEngine AssetExplorer: Another great alternative for Shameless is ManageEngine AssetExplorer (*IT Asset Management Software, ITAM, Asset Lifecycle Management*, n.d.). This is a web-based IT Asset Management (ITAM) software that aids in overseeing and monitoring all the assets in Shamless's network extremely simply from the planning to the disposal phase. Through its IT Asset Inventory Management, the software consistently conducts up to date information through periodically scanning all software, hardware, and ownership information.

3.7 Recording Information about Each Asset

Each asset type has different information being recorded about it. As seen in 3.6.1 of the ISMS, there is certain information that needs to be recorded for the procedures asset type. Please refer to the attached spreadsheet to see what information each asset type requires.

3.8 Evaluating criticality of an asset

In recording each asset, Shameless should largely consider the asset's impact on four areas:

Impact Criterion	**Description**
Cybersecurity	To what extent does the existence, or addition, of this asset affect the company's cybersecurity posture? If the asset was attacked and negatively impacted, how would it affect the rest of the business?
Revenue	To what extent does the existence, or addition, of this asset affect the company's profits?
Image	To what extent does the existence, or addition, of this asset affect the company's reputation among consumers and investors?
Productivity	To what extent does the existence, or addition, of this asset affect the ability of the company and its employees to conduct business?

For each section, provide an integer score from 1 to 10.

Note that all of these areas are interconnected. For example, consider a firewall, which filters incoming network traffic. Therefore we can consider it as highly critical for cybersecurity. If the firewall were to fail, however, and an attacker were to send a barrage of traffic unhindered, employees would be unable to conduct business, therefore impacting productivity, then revenue. The company would then be forced to give public notice that it is facing technical issues and therefore unable to conduct business, potentially impacting its image.

In providing a score for each area, therefore, also consider indirect effects carried over from other areas.

The final step is to calculate the overall criticality of the asset as a weighted average of the scores for each area. For example: cybersecurity could carry 40% weight, revenue could carry 30% weight, image could carry 20% weight, and productivity could carry 10% weight.

Note that **each asset type can, and likely should, have different weight distributions.** For example, more internal assets such as software and hardware would have significant impacts on cybersecurity, but less impact on image. The people of an organization, especially those managers and executives who are the face of the company, can have a large impact on image and, by extension, revenue.

To calculate the weighted average, run the scores through the following formula:
(Here we assume the weight percentage is converted to a decimal from 0 to 1. For example, 50% is equivalent to 0.5.)

```
WEIGHTED_AVERAGE =
  (cybersecurity weight) x (cybersecurity score)
+ (revenue weight) x (revenue score)
+ (image weight) x (image score)
+ (productivity weight) x (productivity score)
```

Consider the following evaluation, for the MySQL database management system:

Impact on Revenue (10%)	Impact on Productivity (40%)	Impact on Cybersecurity (40%)	Impact on Image (10%)	Weighed Score (1-10)
1	8	5	1	?

The weighted score would then be:
(0.1 x 1) + (0.4 x 8) + (0.4 x 5) + (0.1 x 1)
= 5.4

A technical note: In Excel (or Google Sheets), the weighted score can also be calculated as a formula. For example, if the "Impact on Revenue" score of 1 is inputted in cell I2, and the remaining scores are in J2, K2, and L2, then in M2 (the cell where the weighted score will be shown), the following formula can be inserted:

=(0.1 x I2) + (0.4 x J2) + (0.4 x K2) + (0.1 x L2)

4 — Risk Management

4.1 Purpose and Benefits of Risk Management Framework

Information systems play a key role in allowing organizations, such as Shameless, conduct their daily operations. Since Shameless deals with sensitive client data, they must ensure the confidentiality, integrity, and availability of this data while being processed, stored, and transmitted is protected.

There are numerous threats, such as hardware failure, attacks to gain unauthorized access to the systems, and data leakage, that can severely damage Shameless' operations and reputation, lead to high fines, and put sensitive client and employee data at risk. According to NIST Special Publication 800-37, companies like Shameless which deals with Personally Identifiable Information (PII) about their clients should take preventative and corrective measures to protect their systems and manage the risk to their clients (Joint Task Force, 2018). According to the incident reports from the last 12 months provided, however, Shameless lacks such efficient measures, like a working firewall that filters requests or a cohesive incident response procedure, which will help mitigate these risks.

Hence, it's vital that senior management at Shameless, especially the Head of IT, oversee, support, and enable the creation of a Risk Management System. A Risk Management Framework is the process of determining risks to the organization, assessing their impact and magnitude and then responding to the risk by adopting methods to reduce it to an acceptable level (Joint Task Force, 2018). The purpose of a Risk Management Framework is to prevent threats to the organization and its assets and also minimize the impact of said threats through three steps that we will guide Shameless through:

1. **Risk Identification:** The organization identifies and categorizes assets and their threats and vulnerabilities. This requires clear documentation so that the organization can prioritize certain threats over others (see the sheet titled "Risk Management" in the Asset Register attached).
2. **Risk assessment:** After identifying the threats and vulnerabilities, the organization needs to assess its assets' exposure to these risks. The Risk score is calculated via a mathematical formula based on the likelihood of the threat, the

severity of the impact it will have on the organization, current controls and uncertainty value (See section 4.4).

3. **Risk treatment:** Now, the organization will have to identify efficient controls that can mitigate these threats and implement them to reduce risk to an acceptable level.

   Note: Risk can never be completely eliminated, so the aim isn't to reduce risk to 0 but to reduce it to an acceptable level.

There are numerous benefits of adopting a clear and cohesive risk management framework, which will protect the business from threats, without restricting its potential to grow.

Often, the threats can impact the operations of an organization, leading to system downtime. A Risk Management Framework will outline the clear steps that Shameless must take in the case of a disaster and ensure that clients can continue to access the system with minimum downtime. However, without this framework, clients who are unable to utilize Shameless's services may shift to competitors for their insurance needs, as those organizations may have safer platforms with functioning services. Thus, Shameless not only loses revenue due to the loss of clients but also will face reputational damage. These dire consequences can be avoided by having a Risk Management Framework.

Moreover, due to the sensitive nature of the client information Shameless has, there are regulations, such as CCPA and GDPR, that require Shameless to take adequate precautions to protect this information or face legal repercussions and high compliance fines. With a Risk Management Framework, Shameless will maintain the confidentiality and integrity of private client data and meet these requirements, hence we strongly recommend that Shameless creates a Risk Management framework.

4.2 Risk Assessment Methodology and Approach

There are multiple resources available that guide an organization in developing and implementing a Risk Management Framework. Some of the well-known and trusted ones are:

- **ISO 27005:** This is a certification to perform risk management for information security and provides guidelines for risk assessment and treatment. This can be applied to a variety of organizations, irrespective of their size or sector. Since it is a certification, Shameless employees will need to be trained in ISO 27005 in order to implement it in the organization (C-Risk, 2022).
- **OCTAVE:** This framework is used to assess a company's IT environment to determine security risks and plan a risk management system. OCTAVE is broken down in three phases to make it more actionable and easier to implement. Moreover, it is flexible and can be adapted for the needs of different

organizations because there are several variations of the model, ranging from OCTAVE-S, which is appropriate for a team that knows the organization's environment well, to OCTAVE Allegro, which is better for smaller teams (Bigueur, 2015).

- **NIST SP 800-30:** This details steps that organizations need to take to prepare for risk assessments, conduct risk assessments, communicate the results to stakeholders and organizational personnel, and continue and maintain the risk assessment over time. The document specifies and we also emphasize that risk assessment is a continuous process, it cannot be done once. Rather the organization must assess the risk throughout the system development process and document the impact of the controls, so they can be modified to further reduce the residual risk (Joint Task Force, 2012).

We have developed Shameless's system in accordance with NIST SP 800-30 standards. This document is also referred to during the risk identification process to determine threats to and vulnerabilities in Shameless's assets. NIST was an appropriate fit for Shameless for the following reasons:

1. **It is free of cost:** Since Shameless already has a limited budget and has numerous changes that they have to adopt that will take a significant portion of the budget, we thought that we should use NIST, which is free of cost yet is detailed in their recommendations. Hence, we are saving costs without compromising on quality.
2. **It is customizable to the organization:** The NIST framework provides a broad overview of the risk management system and the steps the organization must take to mitigate the negative impact on operations and assets. Under this, the organization can determine what precautions and measures they want to take that meet their needs.
3. **It is scalable:** NIST can be applied to organizations of different sizes. Hence, while Shameless is currently a mid-sized organization when it becomes larger after expanding its business to New Delhi, the company can continue to use NIST to develop and implement its Risk Management framework.

While they are good methodologies, ISO 27005 and OCTAVE aren't appropriate for Shameless right now. ISO 27005 requires employee training, which Shameless will have to dedicate significant resources to do, and currently Shameless lacks the time and budget to obtain this certification. OCTAVE, though comprehensive, is complex to implement compared to NIST, hence the latter is better for Shameless, as most of the staff isn't trained and aware of cyber risks.

4.3 Internal & External Factors of Risks

For Shameless Insurance, the complexities of cybersecurity risks are shaped by a combination of both internal and external factors. Internally, human behavior stands at the front lines, with an immense absence of cybersecurity training and awareness. This can be seen by senior staff falling subject to phishing attacks and the use of weak passwords. Additionally, technical and operational weak points heighten their risk profile (Zero Fox). The use of outdated and/or vulnerable software systems, such as the Apache version 2.2 and an unpatched Microsoft Exchange server, as well as a lack of well-equipped internal monitoring mechanisms, has enabled Shameless to fall prey to malware attacks (Emotet) to exist undetected. This is further heightened by management oversights. The conscious choice to neglect known vulnerabilities, such as Zerologon and PrintNightmare, combined with the lack of regular infrastructure checks points to a reactive rather than a proactive risk management approach. Physical security lapses, demonstrated by device thefts and ineffective disaster recovery during the flood incident, emphasize the extreme need for strengthening tangible security measures. Also, the organizational culture seems to sideline cybersecurity, given the absence of specialized training platforms like a Learning Management Software (LMS).

Externally, Shameless struggles with the fast-evolving threat-technological landscape. This is shown by vulnerabilities in third-party software, like the MOVEit Transfer, which present unforeseen challenges. Regulatory and reputational concerns also linger continuously. Data breaches can quickly result in hefty legal consequences, and as well as the potential reputational backlash from breaches and public media spotlight. In totality, Shameless's cybersecurity landscape is an extremely complicated web of both internal and external dynamics, which amplify and heighten the need for a forward thinking risk strategy.

4.3.1 Quantitative vs Qualitative

Quantitative and qualitative risk assessments both offer unique methods to recognize and understand threats and vulnerabilities within an companies risk landscape.

Quantitative assessments consider the methodology of numerical estimates and values. This method primarily provides objective, and data-driven insights which allows for a more exact computation of potential financial losses. This data aids in prioritizing risk mitigation measures, examining the allocation of resources, as well as enabling measurable metrics to stakeholders NIST Special Publication 800-30.

Qualitative assessments really focus on non-numerical measures, and base evaluations on characteristics and descriptive categories. This method can capture differences, human elements, and organizational culture that otherwise could have been overlooked from a purely number-driven analysis. For Shameless Insurance, given the diverse range of incidents from human error (like phishing email susceptibility) to technical vulnerabilities (like unpatched software), a blended approach might be most suitable. Quantitative analysis would be extremely valuable in understanding the financial consequences of past incidents, such as the $200,000 loss due to mail server issues, a qualitative analysis offers thorough insights into training deficiencies, organizational behavior, and the broader qualitative approach to cybersecurity. Thus, Shameless would benefit most highly from an integrated and cohesive assessment strategy that contains the strengths of both quantitative and qualitative evaluations.

4.3.2 The Effect of Risks

Shameless Insurance and its stakeholders are both greatly affected by risks. Shameless is looking at financial and operational consequences which are highlighted by the substantial monetary losses as well as the tarnishing of its reputation due to cybersecurity lapses. Jointly, stakeholders, such as clients, shareholders, and employees, face the consequences too. Clients unfortunately are subject to having their sensitive data exposed, for example the breaches from Reddit. Shareholders also risk seeing a drop in the value of the company, while employees are simultaneously confronted with job-related uncertainties. Potentially, even third-party partners could experience dips from Shameless's wide array of vulnerabilities (Up Guard). In totality, the company's risk landscape impacts a wide web of everyone connected to it, both internally and externally.

4.3.3 Legal Requirements

If legal requirements are not considered by Shameless Insurance, the consequences will most likely be severe. Disregarding legal orders can most certainly motivate hefty sanctions and fines, which will only add to the company's already hefty financial burdens. Beyond just monetary penalties, non-compliance of the company can result in legal proceedings, which could even further tarnish the company's fragile reputation.

Additionally, inability to meet legal standards may mean that Shameless is running without necessary protections, which in turn leaves client data and other sensitive information extremely open and vulnerable. This can lead to breaches which then attract lawsuits from affected clients or partners. Shameless by eroding its trust with its stakeholders if they do not consider legal requirements because they will most likely distinguish the company as negligent or sloppy. In the long run, non-compliance has the extreme ability to jeopardize the company's license to operate, its business relationships, as well as its overall market position.

4.4 Creating and maintaining a Risk Register

In designing our Risk Register (attached), we follow the principles outlined in ISO 27001 sections 6.1.2 and 6.1.3 for conducting information security risk assessments and risk treatment.

ISO/IEC 27001 — as well as ISO/IEC 27002, which is also referenced in the Risk Register — provide internationally recognized standards and best practices for information security management that, though comprehensive beyond necessity for a smaller company such as Shameless, is still extremely useful. The risk assessment approach in 27001 would help Shameless prioritize security controls based on their specific risk profile. 27002 allows Shameless to implement only the most relevant controls for their size. The standards provide a proven, scalable framework that builds credibility without excessive bureaucracy.

In the longer term, when a stronger culture is established around cybersecurity, Shameless could also look toward obtaining a certification in ISO/IEC 27001 and 27002, pending an official audit based on the standards referenced in this ISMS and others. A certification would demonstrate a strong security commitment to customers and therefore help to repair the company image.

Table 4.1 shows a brief glance at the Risk Register in comparison with ISO 27001:

Table 4.1 Adherence to ISO 27001 standards

ISO 27001 section	Explanation	In Risk Register
6.1.2(a),(b)	establishes a consistent system for assessing risk	- Asset Value - formula for Risk Rating (%)
6.1.2(c)(1)	identify risks associated with the loss of confidentiality, integrity and availability for information	- Vulnerability 1 - Vulnerability 1 Explanation - Vulnerability 2 - Vulnerability 2 Explanation
6.1.2(c)(2)	identify risk owners	- Risk Owner
6.1.2(d)(1)	assess the potential consequences if risks were to materialize	- Exploit - Stakeholders Impacted
6.1.2(d)(2)	quantify the likelihood of the risk occurring	- Vulnerability 1 Likelihood - Vulnerability 1 Likelihood Explanation - Vulnerability 2 Likelihood - Vulnerability 1 Likelihood Explanation
6.1.2(d)(3)	determine the levels of risk	- Risk Rating Vulnerability 1 - Risk Rating Vulnerability 2 - Risk Rating % - Residual Risk
6.1.2(e)(2)	Prioritize the risks for treatment	- Criticality (Color)
6.1.3(a)	select the appropriate risk treatment strategy	- Risk Treatment Strategy

6.1.3(b)	determine the controls necessary to treat the risk	- Recommended Controls - ISO Control (ISO 27002)

The purpose of the Risk Register is to provide a centralized record of key information security risks to the organization. It identifies assets, threats, vulnerabilities, impacts, and controls to manage the risks.

In this section we explain the Risk Register in its entirety, including details about each column.

Notice that the first three columns are the COLOR of the final calculated risk for the asset, the **Asset ID**, and the **Description**. We will return to this criticality color later, once more context is established. The Asset ID and Description are retrieved from the earlier discussed Asset Register. Also note that the **Asset Value** is taken from the Asset Register.

The first column original to the Risk Register is therefore the **Threat**. Here we first consider the definition of a cyber threat — as defined by the National Institute of Standards and Technology (NIST),

> any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service" (*Cyber Threat - Glossary | CSRC*, n.d.).

In short, this requires considering an immediate *event* (as opposed to a technical issue or weakness) that could take place and negatively impact business operations. This event must also, in accordance with ISO 27001 6.1.2(c)(1), be associated with "the loss of confidentiality, integrity and availability for information." In other words, what events could leak information meant to be kept secret (confidentiality)? What events could damage or modify company data (integrity)? What events could result in complete loss of information or shutdown of company services (availability)?

Next, we identify two vulnerabilities that could lead to the Threat; we name these, in no particular order, as **Vulnerability 1** and **Vulnerability 2**. A space is reserved to explain each vulnerability (Vulnerability 1 Explanation, Vulnerability 2 Explanation), which is generally detailing how and why the vulnerability exists and could lead to the threat being actualized. This is continuing the assessment process as outlined in ISO 27001 6.1.2(c), as well as assessing the potential consequences should the vulnerability be exploited, as recommended in ISO 27001 6.1.2(d)(1).

Next, in accordance with ISO 27001 6.1.2(d)(2), we assess the **likelihood** of the vulnerability existing and manifesting as a threat. This would be a scale from 0 to 1. A likelihood of exactly 1 would mean that the vulnerability has already escalated to a threat before. 0.7-0.9 would mean that that has not necessarily happened yet, but it would be extremely likely — and so on and so forth. See Table 4.2 for exact details.

Table 4.2 Determining likelihood of a vulnerability

Likelihood	Description	% likelihood in the next 12 months	Example
0-0.1	**not applicable**	0	will almost never happen, if at all
0.2-0.3	**rare**	5	may happen once every 20 years
0.4-0.5	**unlikely**	25	may happen once every 10 years
0.6-0.7	**moderate**	50	May happen once every 5 years
0.8-0.9	**likely**	75	May happen once every year
1	**certain**	100	may happen multiple times a year

Of course, this is by no means an objective metric; the particular exploit(s) a malicious actor may use is to some degree unpredictable, though, knowing the vulnerabilities of the company's assets, one can make some narrow guesses. This should be treated as more of a gut-instinct metric than anything else. Each input of a likelihood should also then be paired with a **Justification of Likelihood**, which is a brief paragraph explaining what exactly, given the current circumstances of the company, make the vulnerability as likely as was stated.

The next step is to write a potential **Exploit** for each vulnerability, i.e. an example of a technical attack that a malicious client could conduct based on known weaknesses. This would generally be self-evident at this stage, as we have already considered potential exploits in explaining the vulnerability and justifying its likelihood.

Finally, we determine the level of risk presented by each vulnerability, and therefore the total risk presented by each asset — in accordance with ISO 27001 6.1.2(d)(3). First we write out any **Current Controls** that are in place to mitigate the Threat, which, given the current circumstances of the company, are minimal. Then we quantify that as a percentage (0-100). If there are no controls, the **Current Control (%)** is 0.

The **Uncertainty Value (%)** describes how accurate the assumptions and data are. This is our way of acknowledging that we are omniscient about the exact vulnerabilities, exploits and/or financial impacts involved, and factoring in that degree of uncertainty as a quantifiable measure.

Now to calculate the actual risk ratings for each vulnerability. The equation for risk is as follows:

RISK = (Vulnerability Likelihood x Asset Value) - (Current Control %) + (Uncertainty Value %)

Note that each % is taking the percentage of the (Vulnerability Likelihood x Asset Value).

As an example, the following is the calculation for the risk posed by the 2012 R2 server. The asset value is 8.4. Given that, we first calculate the risk of Vulnerability 1 (missing patches) by multiplying 8.4 by the likelihood, which is 1.

8.4 x 1 = 8.4

The current control is 0%, and the uncertainty value is 5% (i.e., we are 95% sure that our assumptions and data are accurate). So we calculate

8.4 - (0% of 84) + (5% of 8.4) = 8.82 ⇐ *Risk Rating of Vulnerability 1*

Similarly, we calculate the risk rating of Vulnerability 2, which also turns out to be 8.82.

We then add [(8.82 + 8.82)/20] * 100 to get the total risk rating percentage.

Since each asset value was out of 10, each risk score should also be out of 10.

We then add the risk scores for each vulnerability to get the total risk value of the asset, which is out of 20. Then we take the percent of this total risk over 20, and display that value. **We therefore get a total risk percentage out of 100 (Risk Rating %).**

Finally: We return to the criticality (color) column we had skipped over earlier. This is achieved by applying conditional formatting based on the total risk percentage we have just calculated, with Table 4.3 as our basis:

Table 4.3 Ranking an asset based on total risk percentage

Rank	Description	Example	Stakeholders Impacted	Productivity Hours Lost	Financial Impact
0-39.99	**Minor (Acceptable Risk Level)**	There is some threat to data but it isn't as significant as other threats and can be mitigated through simple steps	Head of IT	2 hours	$500
40-69.99	**Moderate**	A successful phishing email campaign impacts 10 employees and results in malware being installed on their workstations, leading to potential data theft. The IT, Legal, and HR teams need to investigate, remediate infections, and evaluate damage.	HR, Legal, IT	20 hours	$5,000

70- 84.99	**Major**	A large-scale DDoS attack disrupts customer access for an entire day, impacting sales and therefore revenue. The IT, Sales, and Customer Service teams work urgently to mitigate the attack and restore functionality.	IT, Customers, Sales, HR	200 hours	$50,000
85-100	**Significant**	A data breach results in theft of millions of customer records containing personal identifying information and financial information. This requires notification, remediation, legal and PR response from IT, Customers, Legal, and PR teams. Class action lawsuits are likely from impacted customers.	IT, Customers, Legal, PR, HR, Sales	500 hours	$250,000 plus fines, lawsuits

We have placed the resulting criticality color column as the first column to more immediately establish the level of risk for each asset. These ranks also help to prioritize risks for treatment, in accordance with ISO 27001 6.1.2(e)(2).

The final section of the Risk Register considers the responsibility, impact and treatment of this risk. We first identify the **Risk Owner** in accordance with ISO 27001 6.1.2(c)(2), i.e., who would be responsible for mitigating risk and addressing any events should the listed Threat be realized. Then we consider the **stakeholders** that would be impacted in the event that the Threat is realized, concluding our assessment in accordance with ISO 27001 6.1.2(d)(1).

We then select a **Risk Treatment Strategy**, which is our own terminology for the "appropriate information security risk treatment options" discussed in ISO 27001 6.1.3(a).

Largely speaking, there are five different risk treatment strategies under which to categorize the control(s) for the particular asset: transfer, defense, mitigation, acceptance and termination.

- **Transfer** — shifting the risk to other assets, e.g. outsourcing, purchasing insurance, rethinking how services are offered
- **Defense** — preventing the vulnerability from being exploited, e.g. by proactively adding safeguards and removing the vulnerabilities
- **Mitigation** — drafting a plan to reduce the harm caused by an already realized incident; e.g. incident response (IR), disaster recovery (DR), business continuity (BC) plans
- **Acceptance** — **Not recommended for Shameless**. Deciding to do nothing to protect the asset from risk; this strategy is generally only implemented after

having conducted a thorough cost-benefit analysis and in a certain confidence that the loss or leak of an asset will not cause major damage to the company. In short, the company would simply assume the risk and its consequences.

- **Termination** — **Not recommended for Shameless at this point**. Similar to acceptance, but in this case, refers to a conscious business decision to actively avoid protecting an asset, without regard to its risk. in the future migrate more services to cloud

In most cases, we have recommended a defense strategy to mitigate the risks for each asset. In some cases where we are aware that incidents have already taken place, we have also recommended mitigation and transfer strategies to minimize the harm the company must absorb as a result.

The final few columns are a space to provide **Recommended Controls** for each vulnerability (in accordance with ISO 27001 6.1.3(b)), as well as a justification for each and the relevant section of ISO 27002. There is also a space to quantify the residual risk after having implemented those controls — which is explained further in 4.5.

4.5 Methods of managing risk

Managing risk is extremely crucial for Shameless Insurance, especially following their recent incidents. To mitigate these challenges, Shameless should prioritize regular software updates, enhance employee training, and reinforce their firewall security. Risk transfer, through insurance policies or outsourcing, can also help alleviate potential threats. However, it's essential for the company to understand that not all risks can be eliminated; some must be accepted based on cost or feasibility. Given the company's global operations, diversifying risk and real-time monitoring is vital. After the recent breaches, it's evident that robust incident response planning is essential. Furthermore, considering the phishing incidents, investing in comprehensive employee training is paramount.

Residual risks, which are risks that remain even after mitigation, should be monitored, documented, and revisited periodically to ensure the company's operations align with its risk tolerance NIST Special Publication 800-30. Every year, we suggest that Shameless update the risk register with the residual risk in order to understand if the proposed controls are effective in reducing the risk to an acceptable level (see the residual risk column in the risk register).

5 — Incident Management

5.1 Benefits of an Incident Management System

Incident management is the process by which, in this case, a company responds to an unplanned event or service outage and restores the service to its operational state. One of the primary advantages of implementing an incident management system is the early detection and prevention of issues. By establishing a systematic process for identifying potential incidents, organizations can take preemptive actions to mitigate risks before they escalate into significant disruptions. This early detection capability is crucial in maintaining the stability of crucial business processes. In addition to early detection, incident management policies contribute significantly to minimizing downtime, a critical factor for businesses operating in a competitive landscape. Fast and effective incident response ensures that disruptions are promptly addressed, allowing organizations to resume normal operations and minimize financial losses associated with prolonged downtime. The policy provides a well-defined roadmap for response teams, detailing the steps to be taken to resolve incidents efficiently and effectively. This allows the staff to be able to make well-informed decisions in a time of crisis and in a timely manner. Overall, implementing an IMS is a cost effective plan that will greatly improve the security of Shameless Insurance LTD.

5.2 Incident Management Approach

For Shameless Insurance LTD, we recommend following the standards laid out in the NIST 800-61 Revision 2. When handling an incident, the NIST guidelines take a four step approach. These steps are preparation, detection and analysis, containment, eradication and recovery, and post-incident activity. The first step, preparation, places an emphasis on not only being prepared to respond in case of an incident, but also taking the necessary steps to ensure that incidents are prevented by making sure systems, networks, and applications are sufficiently secure. The second step, detection and analysis, is key because the quicker an incident is detected, the quicker it can be resolved. Because of this, it is imperative that Shameless have measures in place to detect common means of attack. An example would be a properly configured firewall with an intrusion detection/prevention system. Containment, eradication, and recovery is the next step of the process and is based on decision making and willingness to accept risk. As soon as the incident is discovered, it is important to make the decisions necessary to contain the issue and not let it spread, i.e. shutting down a server. With the implementation of an IMS, making these decisions becomes much easier. There are so many factors to consider such as need for evidence preservation, service availability, and duration of the solution. Shameless should also define acceptable risks in dealing with incidents and develop strategies accordingly. After all of the proper controls have been put in place to deal with the problem, Shameless should move into the post incident activity. This involves using the lessons learned and data collected from the incident to prevent it from happening again in the future. Utilizing this method, as opposed to the ISO 27001 is in the best interest of Shameless because NIST offers a more dynamic and fluid approach to dealing with incidents.

5.3 Defining a Security Incident

Defining what constitutes a security incident is fundamental to an effective incident response strategy. At Shameless Insurance, a security incident is defined as any event or occurrence that has the potential to compromise the confidentiality, integrity, or availability of the organization's information assets or information systems. This includes but is not limited to:

Unauthorized access to sensitive customer data or internal systems.

Malicious software infections, including malware, ransomware, or viruses.

Phishing attacks targeting employees or customers.

Insider threats, including data breaches by employees.

Physical security breaches, such as unauthorized access to facilities or equipment.

Denial of Service (DoS) attacks disrupting service availability.

Defining security incidents with precision allows the organization to categorize, prioritize, and respond to them effectively.

5.4 Classifying a Security Incident

To ensure a structured and efficient response to security incidents, Shameless Insurance classifies incidents based on their severity and potential impact. The classification levels include:

Critical Incidents: Incidents that pose an immediate and severe threat to the organization's operations, customer data, or reputation. These incidents require an urgent and comprehensive response.

High-Priority Incidents: Incidents with a significant potential impact but not as severe as critical incidents. High-priority incidents demand prompt attention and specialized response efforts.

Medium-Priority Incidents: Incidents that have the potential to cause moderate disruption or damage. These incidents are addressed in a timely manner but may not require immediate attention.

Low-Priority Incidents: Incidents with minimal potential impact that do not pose an immediate threat. These incidents are addressed as resources permit.

The classification of security incidents helps in allocating resources effectively and ensuring that the most critical threats are addressed promptly.

5.5 Identifying and Reporting Incidents

Identifying and reporting incidents promptly is crucial to the incident response process. Shameless Insurance encourages all employees and stakeholders to report any suspicious activity or potential security incidents immediately. Incident identification and reporting methods include:

Employee training on recognizing security threats and incidents.

Clear reporting channels and contact points for employees.

Automated monitoring tools and intrusion detection systems.

Regular security awareness campaigns to raise incident reporting awareness.

An incident reporting form or system for external parties and customers.

All reported incidents are treated seriously, and a consistent process is followed for assessment and response.

5.6 Performance Metrics

In all aspects of business, measuring performance metrics are key in improvement and innovation of the company. This is especially true when it comes to incident management. Accurate and comprehensive data on the types and frequency of incidents provides invaluable insights, serving as a guideline for devising proactive strategies to prevent and recover from such events seamlessly. By scrutinizing the metrics associated with incidents, businesses can identify patterns, vulnerabilities, and potential areas for enhancement in their existing systems and processes. The continuous measurement of performance metrics in incident management is not merely a procedural formality; rather, it is an integral component of the business that propels the organization towards a state of greater preparedness and adaptability. The measurement of these data points is not a one-size-fits-all approach; rather, it necessitates an extensive integration across all levels of the business, with particular emphasis on post-incident activities. Once an incident has been resolved, it becomes a lesson to learn from. By logging and storing all of the data from these events, Shameless will be able to mitigate future incidents from occurring.

5.7 Documenting Incidents

Proper documentation of security incidents is essential for analysis, reporting, and continuous improvement. At Shameless Insurance, the following documentation practices are followed:

- Incident Reports: Detailed reports are created for each incident, including incident classification, impact assessment, incident timeline, and actions taken.
- Evidence Preservation: Any digital evidence related to the incident is preserved in accordance with legal and regulatory requirements.
- Lessons Learned: After each incident is resolved, a post-incident review is conducted to identify lessons learned, improvements in incident response procedures, and potential preventive measures.
- Incident Logs: Comprehensive incident logs are maintained for historical reference and trend analysis.
- Regulatory Reporting: Documentation is provided as required by relevant regulatory bodies, ensuring compliance with data breach notification requirements.

By documenting incidents systematically, Shameless Insurance can learn from past experiences, strengthen incident response capabilities, and continually enhance its overall security posture.

5.8 Roles of CPMT, IRT

Fig 5.8.1 Flow diagram showing roles and responsibilities within CPMT. The COO heads the team, considering in totality the business operations that should remain up in the case of an incident, with each of the other departments considering different aspects of said operations.

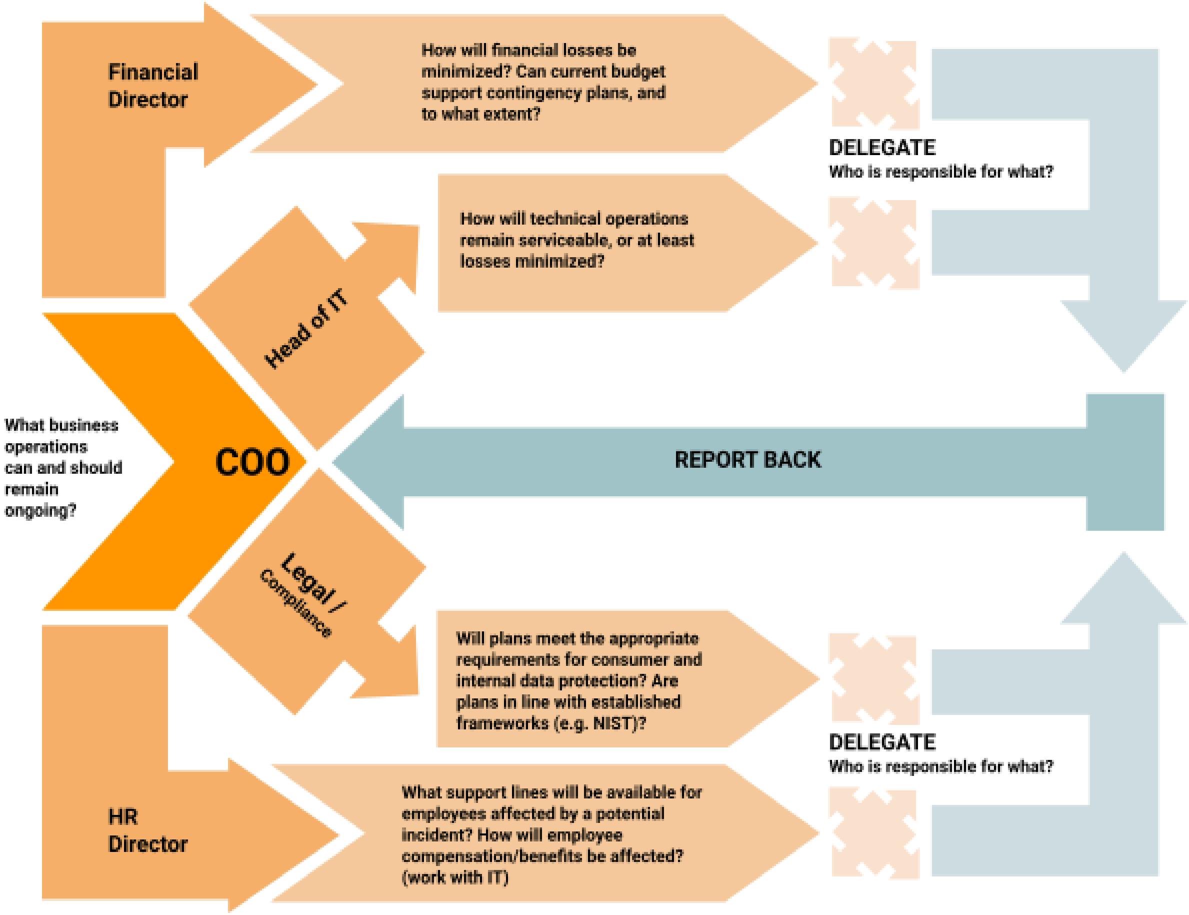
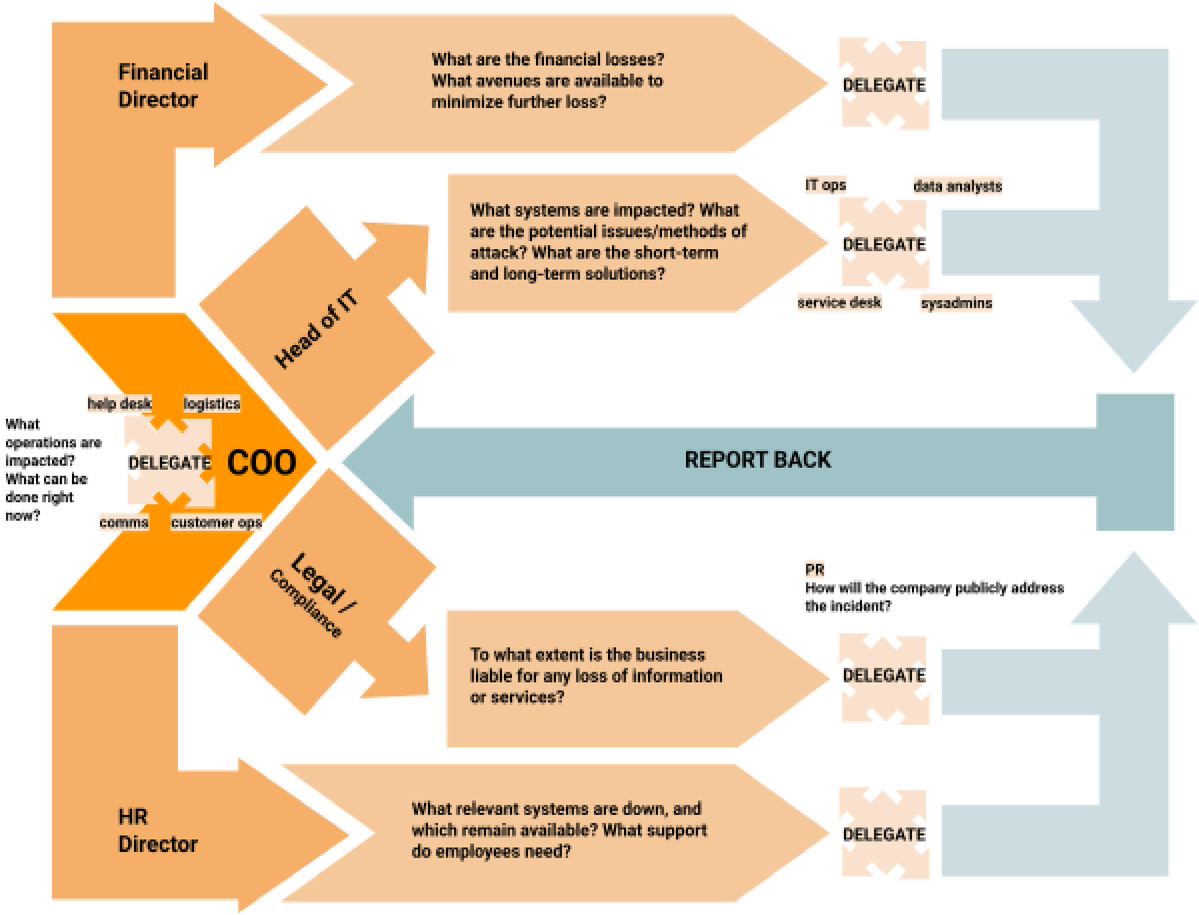

Financial Director
How will financial losses be minimized? Can current budget support contingency plans, and to what extent?
DELEGATE
Who is responsible for what?
Head of IT
How will technical operations remain serviceable, or at least losses minimized?
What business operations can and should remain ongoing?
COO
REPORT BACK
Legal / Compliance
Will plans meet the appropriate requirements for consumer and internal data protection? Are plans in line with established frameworks (e.g. NIST)?
DELEGATE
Who is responsible for what?
HR Director
What support lines will be available for employees affected by a potential incident? How will employee compensation/benefits be affected? (work with IT)

Fig 5.8.2 Flow diagram showing roles and responsibilities within IRT. All departments report back to COO, but each department ultimately has its separate hierarchy through which issues and solutions will be communicated bottom-up. The COO oversees their own department, as well as the general response across all other departments without any more involvement than is needed regarding the details.


Financial Director
What are the financial losses? What avenues are available to minimize further loss?
DELEGATE
IT ops
data analysts
What systems are impacted? What are the potential issues/methods of attack? What are the short-term and long-term solutions?
DELEGATE
service desk
sysadmins
Head of IT
help desk
logistics
What operations are impacted? What can be done right now?
DELEGATE
COO
comms
customer ops
REPORT BACK
Legal / Compliance
PR
How will the company publicly address the incident?
To what extent is the business liable for any loss of information or services?
DELEGATE
HR Director
What relevant systems are down, and which remain available? What support do employees need?
DELEGATE

5.9 Examples

As an example, we consider the past incident in which the business's MOVEit Cloud file management system was exploited via the MOVEit Transfer Vulnerability (CVE-2023-35708).

At the contingency planning stage, the COO should see to it that the files of each department are backed up in an alternative location besides the cloud, ideally in hard storage. The Head of IT would then create a procedure to restore those backups in the event of an incident, and check with Legal/Compliance to ensure that said procedures are in line with data protection law.

Each department should then be informed as to what steps its employees should take to participate in the backup procedure — that information distributed by Compliance and HR.

Head of IT should also be the one to notice that the MOVEit Cloud version had that vulnerability, and report that directly to the COO.

At the incident response stage, the Head of IT would likely be the first to notice a breach, having received a report through the ranks thanks to a detection system that would ideally be in place. This would then be alerted to the COO, who would then initiate the incident response procedure. Head of IT would analyze and report the exact losses in data, and work to restore backups and set up immediate alternate workflows as planned.

Each department would then read through the data loss report and see what data has been lost; and also report what data they notice has also been lost or damaged. HR would step up its employee support lines, and ensure that relevant systems are still intact. Legal and Compliance would assess the extent to which the breach would violate existing laws and frameworks; Financial would assess the financial extent of the loss.

Head of IT, having assessed the situation, would come up with, and distribute, a temporary solution to keep the business operating at a minimum level, and a patch for the technical issues. These findings would then be reported in totality to the COO, as well as intermittently as the situation progresses.

6 — Policies and Procedures

As part of establishing a comprehensive information security management system, we recognize Shameless Insurance Ltd's need for a layered approach to provide direction, set technical controls, influence staff behaviors, and drive specific actions that support the organization's information security risk posture. To achieve these outcomes, the ISMS establishes crucial security policies, implements supporting technical security standards, promotes recommended security best practices, and defines procedural workflows to execute localized security responsibilities.

6.1 Definitions of Terms

6.1.1 Policies

Policies provide high-level statements and principles to set the direction and expectations for the organization's security posture. They communicate the "what" needs to be done, but not the details of how. Policies should be accessible and understandable to the managers and executives who need to enforce them; they should also be such that Legal and Compliance would be convinced they are aligned with current laws governing data privacy and information security, e.g. GDPR (**1.6.1**) and CCPA (**1.6.2**). Note, however, that policies should be absent of technical specifications; those are best left for standards (**6.2**) and procedures (**6.4**).

6.1.2 Standards

The intended audience for security standards are technical teams and IT staff. Standards provide specific technical requirements, configurations, reference architectures, approved tools/technologies to implement the principles set out in policies across the organization's systems and services. They focus on the "how" for security controls and implementations. Standards are written for the IT and Operations departments. Standards should be aligned with existing frameworks offered by ISO 27001.

6.1.3 Best Practices

Best practices describe recommended secure behaviors and methods for protecting information and technology resources based on research and expertise. They inform employees what they should do to enhance security, providing more practical "how-to" advice to support policy principles and technical standards. These are intended for all employees in the organization without exception.

6.1.4 Procedures

Procedures lay out step-by-step implementation instructions for security processes and controls. Procedures give detailed workflow guidance on exactly how to execute security tasks to meet standards and policies tailored to each environment. They are more tailored toward specific departments: each department by definition has vastly different workflows which require specially tailored security tasks and controls; in the event of a breach or other cybersecurity incident, each department must also have a unique procedure to recover business operations and minimize damages to the organization.

6.2 Policy Justification

Shameless Insurance's rapid growth has exposed gaps in consistent security direction across the organization. As evident by redundant issues like unpatched systems and reused credentials enabling preventable breaches, Shameless lacks formal policies and accountability mechanisms to govern security programs. By codifying baseline expectations and compliance requirements within information security policies, Shameless can proactively mitigate root causes rather than continually reacting to incidents.

Well-defined policies cascade from the top-down to align all staff to the same security objectives. They translate abstract concepts like "protecting data" into reviewable business logic and technical controls. Given repeated struggles getting line staff and remote offices on the same page security-wise, corporate policies provide a straight-forward means to disseminate the CEO's and Board's priorities. Recent client losses suggest Shameless specifically needs policy visibility to ensure all personnel uphold expected standards regardless of geography or reporting structure. Information security policies also serve as an audit point during incidents to evaluate if inadequate controls contributed to an event by violating policy tenets.

By evaluating the ISMS against defined policies, any gaps can then be addressed at their core through revised policy statements rather than just responding to impacts. For Shameless to show good faith security progress to partners after high-profile incidents, embracing security policies represents both a strategic and tactical solution.

6.3 Policy selections

Security Frontline has decided upon the following four policies to recommend foremost, though this is absolutely not an exhaustive list Shameless could certainly benefit from several others:

- Secure Password Policy (**6.3.1**)
    - *Procedure: Enrolling in Okta Multi-Factor Authentication*
- Software Update and Patch Management Policy (**6.3.2**)
- Bring Your Own Device Policy (**6.3.3**)
- Backup and Recovery Policy (**6.3.4**)

We have attached a sample Secure Password Policy and Bring Your Own Device Policy to this document for reference, as well as an Okta Multi-Factor Authentication enrollment procedure as an addendum to the Secure Password Policy.

Formalizing these core policies provides a consolidated approach to instill baseline controls rather than relying purely on technical solutions. These policies govern both employee practices and technical configurations, such that all employees can be involved in the company's cybersecurity posture — which will aid greatly in much-needed cybersecurity awareness within Shameless. With major clients already lost and others openly doubting Shameless's security commitment after breaches, these policies tackle publicized deficiencies at the root by universally regulating security hygiene. We believe it is these policies specifically that will most benefit Shameless in rebuilding trust, and establishing a proper culture around information security, before pursuing more advanced controls elsewhere within the ISMS.

6.3.1 Secure Password Policy

Given Shameless Insurance's demonstrable weaknesses regarding passwords, which have led to severe breaches of the company, having a password policy is of utmost importance. The following table lists the benefits of having a Secure Password Policy, as well as the justifications for each benefit:

Table 6.3.1.1 — Benefits

Benefit	**Justification**
Prevents unauthorized access	Enforcing password complexity and regular rotation prevents attackers from easily guessing or cracking user credentials to access systems and

	data.
Reduces risk of account compromise	Requiring frequent password changes and prohibiting reuse limits exposure if passwords are phished or otherwise obtained by bad actors.
Regulatory compliance	Password controls align with data security standards like PCI DSS, which require multilayer authentication protections.
Identity confirmation	Combining passwords with secondary factors like biometrics and security keys provides stronger identity verification and reduces malicious login attempts.
Promotes employee security awareness	Mandating secure password habits serves to force staff to follow best practices and take ownership of account protections.

Table 6.3.1.2 — ISO 27001 compliance

ISO 27001 control	**Description**	**Justification**
A.5.17 *Authentication information*	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	This control covers the allocation and management of authentication information, including advising personnel on appropriate password handling. The password policy defines requirements for proper password practices.
A.8.2 *Privileged access rights*	The allocation and use of privileged access rights shall be restricted and managed.	The password policy restricts and manages access rights by enforcing password controls, especially for privileged user accounts.
A.8.5 *Secure authentication*	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	This control stipulates implementing secure authentication technologies and procedures based on access restrictions. The password policy puts technology and rules in place to improve authentication.

6.3.2 Software Update & Patch Management Policy

Shameless has several softwares that are out of date and/or need to be patched, leaving them openly vulnerable to exploits that can severely damage the organization, its data, and its reputation.

Table 6.3.2.1 — Benefits

Benefit	**Justification**
Reduces attack surface	Rapidly patching known system vulnerabilities mitigates the window of exposure for attackers to exploit them to gain access.
Limits malware impact	Keeping software up-to-date closes security holes targeted by malware attacks before incidents can spread.
Improves resilience	Applying updates to repair software faults improves system reliability and prevents instability issues.
Demonstrates due diligence	Having a patch policy displays security diligence to clients if audited after a software-related breach.
Enables central control	Centralized patch management allows efficient, enterprise-wide rollouts rather than relying on individual user compliance.
Simplifies version tracking	Automated patches facilitate software license and version management with a consistent baseline.

Table 6.3.2.2 — ISO 27001 compliance

ISO 27001 control	**Description**	**Justification**
A.8.8 *Management of technical vulnerabilities*	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	Keeping software updated with the latest vendor patches addresses known technical vulnerabilities in systems that could allow attackers to gain access.
A.8.34 *Protection of information systems during audit testing*	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	Patch testing via audit scans helps validate that patches were applied appropriately without impeding operations.

***A.8.32** Change management*	Changes to information processing facilities and information systems shall be subject to change management procedures.	This current policy ensures a controlled change management process for updating business-critical systems.

6.3.3 Bring Your Own Device Policy

Lack of a comprehensive BYOD policy has led to a notably weak cybersecurity culture which has exposed Shameless to a number of vulnerabilities. Implementing a comprehensive policy in this regard will greatly strengthen Shameless's cybersecurity profile while still maintaining the level of flexibility that employees have come to expect in their workflows, with minimal transition required and associated cost greatly reduced.

Table 6.3.3.1 — Benefits

Benefit	**Justification**
Increases flexibility	Allowing personal mobile devices provides more options for employees to securely access corporate resources remotely.
Enables mobility	Authorizing BYOD opens up access from anywhere to improve productivity for the mobile sales force.
Reduces costs	Leveraging employee-owned devices reduces organizational capital spending on providing devices.
Simplifies administration	Centrally enforcing policies, configurations, and controls through software such as a unified endpoint management platform (UEM) is easier than trying to secure BYODs individually.

Table 6.3.3.2 — ISO 27001 compliance

ISO 27001 control	**Description**	**Justification**
***A.6.2** Terms and conditions of employment*	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	Defines BYOD policy responsibilities for employees and the company.
***A.8.1** User endpoint devices*	Information stored on, processed by or accessible via user end point devices shall be protected.	Ensures BYOD devices are properly secured to protect company data.

A.8.2 *Privileged access rights*	The allocation and use of privileged access rights shall be restricted and managed.	Limits privileged access on BYOD devices to authorized purposes.
A.6.7 *Remote working*	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Policy specifies that BYOD devices are still restricted regardless of working remote or in the office
A.13.2.1 *General*	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Requires regular backups and testing for recovery of BYOD device data.

6.3.4 Backup and Recovery Policy

This is only one section, though arguably one of the most important, of a comprehensive disaster recovery policy which we highly recommend Shameless develop and implement. In the event that data is lost due to circumstances out of the company's control, having a plan to restore as much of that data as possible will greatly reduce damages, both to Shameless's finances and reputation.

Table 6.3.4.1 — Benefits

Benefit	**Justification**
Prevent permanent data loss	Backups ensure company data can be recovered in case of hardware failure, data corruption, malicious attacks, or accidental deletion
Minimize downtime after failures	Quickly restoring data from backups reduces system unavailability
Regulatory compliance	Backups satisfy legal requirements for retaining and being able to produce business records
Enhanced cyber resilience	Secure offsite backups facilitate recovery from ransomware and other cyber incidents

Table 6.3.4.2 — ISO 27001 compliance

ISO 27001 control	**Description**	**Justification**

A.8.2 *Privileged access rights*	The allocation and use of privileged access rights shall be restricted and managed.	Limits privileged access to backups to prevent unauthorized access or tampering.
A.8.13 *Information backup*	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Ensures regular backup of critical systems and data along with testing backup recoverability.
A.17.1 *Physical security perimeters*	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Backup media must be stored securely to prevent theft or damage.
A.18.1.3 *Securing offices, rooms and facilities*	Physical security for offices, rooms and facilities shall be designed and implemented.	Backup facilities must be physically secured against unauthorized access.

SECURE PASSWORD POLICY

Jonathan Park

Security Frontline

for client:

Shameless Insurance Ltd

Version Control

Date	**Author**	**Version**	**Description**
10 Dec 2023	Jonathan Park	1.0.0	Created
11 Dec 2023	Jonathan Park	1.1.0	Minor edits
12 Dec 2023	Jonathan Park	1.1.1	Minor edits

This Secure Password Policy was drafted in part using the SANS Institute's Password Protection Policy, which is freely available for use and distribution.

1 — Overview

Passwords are a critical aspect of computer security. A weak or compromised password can result in unauthorized access to our most sensitive data and/or exploitation of our resources. All staff, including contractors and vendors with access to Shameless Insurance Ltd ("Shameless") systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

1 — Purpose

This policy establishes secure password requirements for Shameless systems and devices. Proper password controls prevent unauthorized access and account compromise, enabling us to protect sensitive customer data.

2 — Scope

This policy applies to all Shameless personnel with access privileges to company systems and devices, including:

- Servers, workstations, laptops
- Mobile devices
- Software applications
- Cloud-based services

3 — Policy

Shameless passwords must adhere to the following standards:

Password Complexity

- 12-24 characters
- Combine upper and lowercase letters
- Include one or more number
- Include one or more symbols (e.g. @ # $ %)

- Passwords may not contain easily guessable words or phrases, especially phrases that can be associated with Shameless Insurance, or personal information such as birthdays or names of loved ones

Password Changes

- All employees will be required to change their passwords to company softwares and employer-provided devices every 12 months, generally at the conclusion of each Fiscal Year barring extenuating circumstances or other exceptions.

- None of the previous five passwords used by the same user will be allowed as the new password.

Lockout Policies

- 10 failed login attempts will require password reset, with email verification required.

Multi-factor Authentication

- All employees at every level will be required to enable at least two-factor authentication with Okta.

- Privileged employees with access to sensitive internal or customer data will be required to enable multi-factor authentication, with a push notification sent through Okta and a verification code sent to the user's work email.

Storage Requirements

- Encrypt passwords during transmission and storage.

- Prohibit plaintext password storage in any medium or capacity, including the notes app on a user's device, a virtual document, stickied paper in plain view in the office, etc.

- Storing passwords in a third-party password manager such as LastPass is acceptable but not recommended.

- Do not use the "Remember Password" feature of any web browser or application (Safari, Chrome, Firefox, iCloud KeyChain, etc.)

4 — Password sharing

- Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, confidential Shameless information.

- Passwords must not be inserted into email messages or other forms of electronic communication, nor revealed over the phone to anyone.

- Passwords may be stored only in password managers authorized by the organization.

Any individual suspecting that their password may have been compromised must report the incident to Shameless IT and change all relevant passwords.

5 — Policy Compliance

Compliance Measurement

Shameless IT will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

Non-Compliance

Passwords found to be in violation of the Password Complexity requirements will be sent a password reset link; after three violations of these requirements, the employee will be required to retake compliance training material concerning this Policy.

Any employee found to have violated any other terms of this policy may be subject to disciplinary action, up to and including termination of employment.

6 — Related policies and procedures

- Procedure: Enrolling in Okta Multi-Factor Authentication

BRING YOUR OWN DEVICE (BYOD) POLICY

Jonathan Park

Security Frontline

for client:

Shameless Insurance Ltd

Version Control

Date	Author	Version	Description
10 Dec 2023	Jonathan Park	1.0.0	Created
11 Dec 2023	Jonathan Park	1.1.0	Minor edits
12 Dec 2023	Jonathan Park	1.1.1	Minor edits

This Bring Your Own Device policy was drafted in part using Workshop's BYOD Policy & Agreement template.

1 — Definitions

Bring Your Own Device (BYOD): Privately owned wireless and/or portable electronic handheld equipment.

2 — Overview

This policy establishes Shameless Insurance Ltd's guidelines for employee use of personally owned electronic devices for work-related purposes.

Acceptable use of BYOD at Shameless must be managed to ensure that access to Shameless's resources for business are performed in a safe and secure manner for participants of the Shameless BYOD program. A participant of the BYOD program includes, but is not limited to:

- Employees
- Contractors
- Related constituents who participate in the BYOD program

2 — Purpose

This policy establishes requirements for the use of personal mobile devices to process, store, or transmit Shameless Insurance data. The intent is to minimize security risks from BYOD while providing convenient remote access.

3 — Scope

This policy applies to all Shameless employees, contractors, and other personnel with access privileges to company data or networks via personally-owned mobile devices, including. but not limited to:

- Smartphones
- Tablets
- Laptops
- Related software that could be used to access corporate resources

4 — Policy

4.1 Security and Safety

To ensure the security of Shameless information, authorized employees are required to have antivirus and mobile device management software installed on their personal mobile devices. This mobile device management software will store all company-related information, including calendars, e-mails and other applications in one area that is password-protected and secure. Shameless IT must install this software prior to using the personal device for work purposes.

Employees may store company-related information only in this area. Employees may not use cloud-based apps or backup that allows company-related data to be transferred to unsecure parties. Due to security issues, personal devices may not be synchronized with other devices in employees' homes. Making any modifications to the device hardware or software beyond authorized and routine installation update is prohibited unless approved by Shameless IT. Employees may not use unsecure Internet sites.

We also require all employees to adhere to the following security protocols:

- In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.

- Employees must adhere to the Shameless Secure Password Policy.

- Employees are automatically prevented from downloading, installing, and using any app that does not appear on the company's list of approved apps.

- Smartphones and tablets that are not on the company's list of supported devices are/are not allowed to connect to the network.

- Smartphones and tablets belonging to employees that are for personal use only are/are not allowed to connect to the network.

- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.

- The employee's device may be remotely wiped if 1) the device is lost, 2) the employee terminates their employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

4.2 Shameless IT reserves the right to:

- Centrally manage the BYOD program and devices including onboarding approved users, monitoring BYOD connections, and terminating BYOD connections to Shameless resources upon employee separation
- Manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable
- Refuse, by non-physical means, the ability to connect mobile devices to Shameless infrastructure if such equipment is deemed a security risk
- Maintain a list of approved mobile devices and related software applications and utilities. Unapproved devices may not connect to Shameless infrastructure
- Maintain enterprise IT security standards
- Inspect all mobile devices attempting to connect to the Shameless network through an unmanaged network using centrally managed technology
- Install any and all software IT deems necessary and reasonable to conduct business operations, with this list of software having undergone managerial approval
- Restrict applications
- Limit use of network resources
- Wipe data on lost/damaged devices or upon termination from the BYOD program or Shameless employment
- Limit, through policy enforcement and any other means, the ability of end users to transfer data to and from specific Shameless network resources

4.3 Lost, stolen or damaged devices

Shameless will not be responsible for loss or damage of personal applications or data resulting from the use of company applications or the wiping of company information.

Employees are expected to protect personal devices used for work-related purposes from loss, damage or theft.

Employees must have “remote-wipe” software installed on their BYOD devices by the IT department prior to using the devices for work purposes.

Lost, stolen or damaged devices must be reported immediately to Shameless IT — at most 24 hours after the loss or damage occurs and/or is noticed.

If the device is lost or stolen, Shameless IT may then begin to wipe the device completely of its contents (see sections 4.1, 4.2). Wiping company data may affect other applications and data.

If the device is damaged, Shameless IT may attempt to repair the device. If IT is unable to repair the device, the employee will be responsible for the cost of replacement. Neither Shameless or its IT department will be responsible for any damages caused while attempting to repair the device.

Employees may receive disciplinary action up to and including termination of employment for damage to personal devices caused willfully by the employee. Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT. Non-sanctioned use of mobile devices to backup, store, and otherwise access any enterprise-related data is strictly forbidden.

This policy is complementary to any other implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the Shameless network.

4.4 Termination of employment

Upon resignation or termination of employment, or at any time on request, the employee may be asked to produce the personal device for inspection. All company data on personal devices will be removed by IT upon termination of employment

5 — Compliance

Employees who have not received authorization in writing from [Company Name] management and who have not provided written consent will not be permitted to use personal devices for work purposes.

Shameless IT will regularly and without warning audit registered BYOD devices for compliance.

Failure to follow Shameless policies and procedures may result in disciplinary action, up to and including termination of employment.

6 — Related policies and procedures

- Secure Password Policy

ENROLLING IN OKTA TWO-FACTOR AUTHENTICATION (MFA)

SECURITY
FRONTLINE

Jonathan Park

Security Frontline

for client:

Shameless Insurance Ltd

Version Control

Date	**Author**	**Version**	**Description**
10 Dec 2023	Jonathan Park	1.0.0	Created
11 Dec 2023	Jonathan Park	1.1.0	Minor edits
12 Dec 2023	Jonathan Park	1.1.1	Minor edits

1 — Definitions

Multi-factor authentication (MFA) is an access control security mechanism that requires users to present two or more credentials, categorized into independent factors of authentication, to gain access to IT resources, systems, networks, devices, or applications.

The three basic factors available for authentication are:

- Knowledge - Something the user knows, like a password or PIN
- Possession - Something the user physically has, like a token or badge
- Inherence - A user's inherent biometric trait, like a fingerprint

By requiring two or more of these factors to successfully authenticate, MFA enhances security as gaining unauthorized access requires an attacker to independently compromise or hijack additional proof of identity. For instance, if an attacker phished a password (knowledge factor), they still could not login without also obtaining and presenting the user's biometrics (inherence factor) captured by a separate scanner device. MFA is therefore used as an additional layer of information security to better vet and control access within organizations.

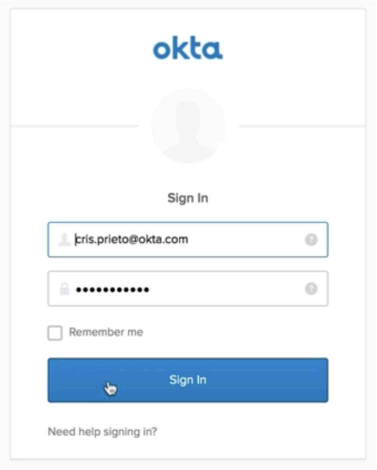
Okta is the particular software Shameless will be using for its multi-factor authentication.

2 — Procedure

2.1 Enrolling in Okta Verify Push

For a video version, watch the official video tutorial by Okta.

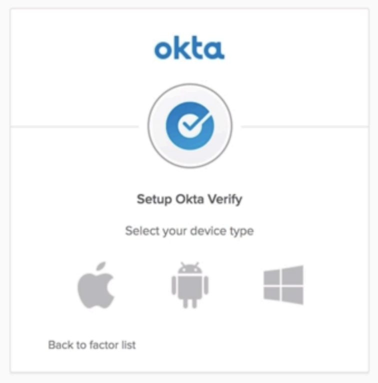
Navigate to the usual login page; you may notice that the portal login screen now directs you to login via Okta. **Your credentials should remain unchanged;** log in as usual.



cris.prieto@okta.com

•••••••••••

You will then be directed to this screen. Select the type of device for your *smartphone*: (from left to right) Apple (iPhone, iPad), Android (Samsung, LG or any other), or Windows (Windows Phone).



okta

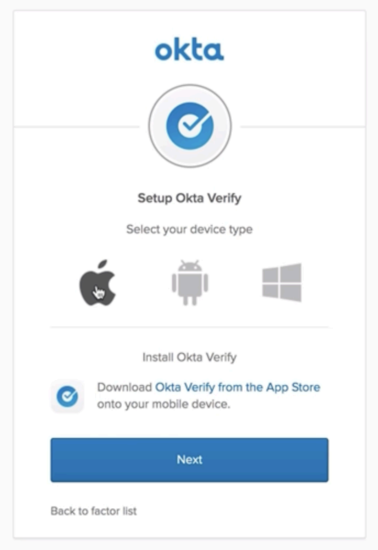
Setup Okta Verify

Select your device type

Back to factor list

The directions from here on should be virtually identical regardless of the type of device, with only minor differences.

Once you select the device, you should be directed to download the Okta Verify app on your phone.



okta

Setup Okta Verify

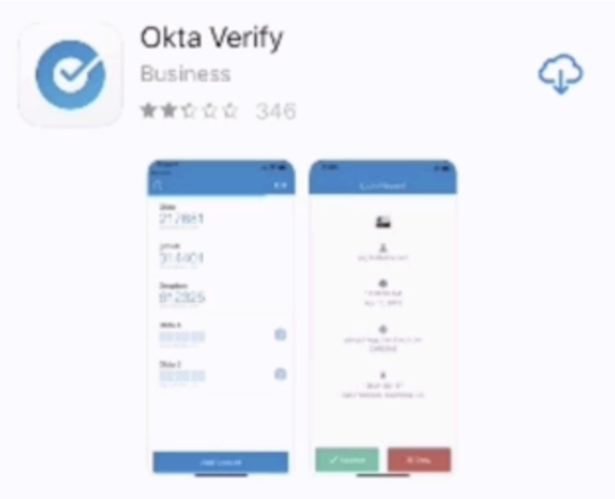
Select your device type

Install Okta Verify

Download Okta Verify from the App Store onto your mobile device.

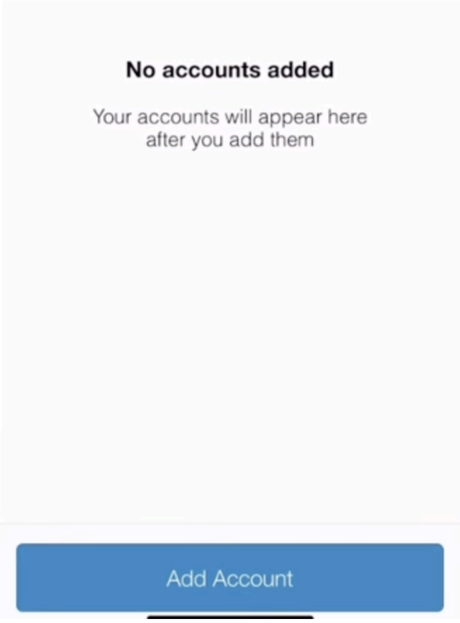
Next

Back to factor list



Once the Okta Verify app is installed, open the app.

You will then be prompted to “Add Account.” Tap “Add Account.”



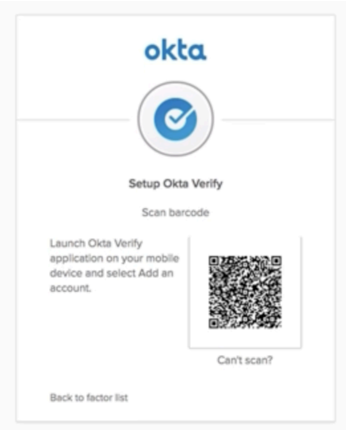
No accounts added

Your accounts will appear here after you add them

Back on the computer, click “Next.” It should display a QR code. The Okta Verify app on your phone should have opened the phone camera to scan the QR code. Scan the QR code.

An account should then be added to the Okta Verify app.

computer

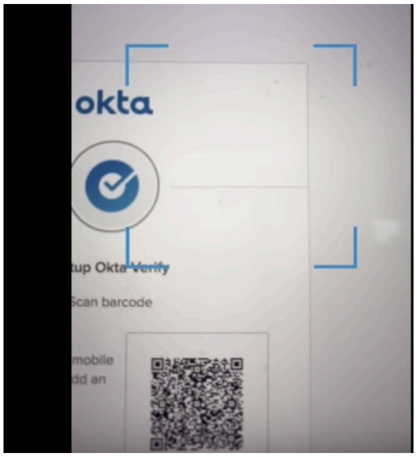


Setup Okta Verify

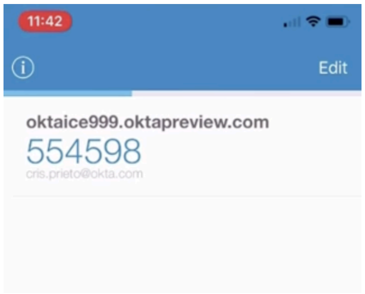
Scan barcode

Launch Okta Verify application on your mobile device and select Add an account.

phone screen



result on phone



oktaice999.oktapreview.com

554598

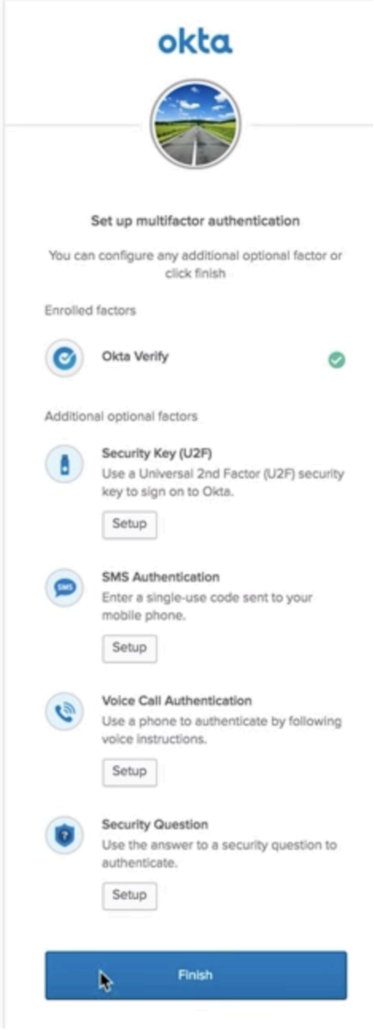
cris.prieto@okta.com

Great! Now, whenever you log in, you will first be sent a push notification to this Okta Verify on your phone, that you will have to tap and confirm that it is you who is logging in.

Note that this is just two-factor authentication so far. Continue to the third factor …

2.2 Set up multi-factor authentication

On your computer, you will automatically be redirected to this screen.



Set up multifactor authentication

You can configure any additional optional factor or click finish

Enrolled factors

Okta Verify

Additional optional factors

Security Key (U2F)
Use a Universal 2nd Factor (U2F) security key to sign on to Okta.

SMS Authentication
Enter a single-use code sent to your mobile phone.

Voice Call Authentication
Use a phone to authenticate by following voice instructions.

Security Question
Use the answer to a security question to authenticate.

For users requiring two-factor authentication, you may simply press Finish.

For other users requiring multi-factor authentication, select any of the four available options and follow the instructions.

References

About Asset Panda. (n.d.). Asset Panda. Retrieved September 28, 2023, from https://www.assetpanda.com/our-company/

Bernard, J., Golden, D., Nicholson, M., & Baviera, R. (2020, July 24). *Reshaping the cybersecurity landscape*. Deloitte. Retrieved September 28, 2023, from https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html

Bigueur, M. (2015, August 2). *Risk Assessment Methodologies*. Bigueur's Blogosphere. Retrieved October 26, 2023, from https://miguelbigueur.com/2015/08/02/risk-assessment-methodologies/

C-Risk. (2022, March 3). *ISO 27005: everything you need to know if you are considering implementing it*. C-Risk. Retrieved October 26, 2023, from https://www.c-risk.com/en/blog/iso-27005/

Cyber Threat - Glossary | CSRC. (n.d.). NIST Computer Security Resource Center. Retrieved October 29, 2023, from https://csrc.nist.gov/glossary/term/Cyber_Threat

Data Protection Compliance for Insurance Companies. (2023, April 12). Ekran System. Retrieved December 11, 2023, from https://www.ekransystem.com/en/blog/data-protection-compliance-insurance-industry

How Often Should You Change Your Passwords? (n.d.). McAfee. Retrieved December 11, 2023, from https://www.mcafee.com/learn/how-often-should-you-change-your-passwords/

IT Asset Management Software, ITAM, Asset Lifecycle Management. (n.d.). ManageEngine. Retrieved September 28, 2023, from https://www.manageengine.com/products/asset-explorer/

IT Asset Management Software, ITAM, Asset Lifecycle Management. (n.d.). ManageEngine. Retrieved September 28, 2023, from https://www.manageengine.com/products/asset-explorer/

Joint Task Force. (2012, September). *NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments*. NIST Technical Series Publications. Retrieved October 26, 2023, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Joint Task Force. (2018, December 2). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. NIST Technical Series Publications. Retrieved October 26, 2023, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Lineman, D. (2011, January 20). *What is the difference between security policies, standards and procedures?* Information Shield. Retrieved December 11, 2023, from https://informationshield.com/2011/01/20/what-is-the-difference-between-security-policies-standards-and-procedures/

Loshin, D. (n.d.). *What are Data Structures? - Definition from WhatIs.com*. TechTarget. Retrieved September 28, 2023, from https://www.techtarget.com/searchdatamanagement/definition/data-structure

Nash, A. (2023, May 25). *External Threats vs. Internal Threats in Cybersecurity*. ZeroFox. Retrieved October 27, 2023, from https://www.zerofox.com/blog/external-threats-vs-internal-threats-in-cybersecurity/

National Protective Security Authority. (2020, February 17). *Policies, Standards, Guidelines & Procedures | NPSA*. National Protective Security Authority. Retrieved December 11, 2023, from https://www.npsa.gov.uk/insider-risks/policies-standards-guidelines-procedures

Pearson IT Certification. (2002, December 20). *Classifying Data | CISSP Security Management and Practices*. Pearson IT Certification. Retrieved September 25, 2023, from https://www.pearsonitcertification.com/articles/article.aspx?p=30287&seqNum=9

Ross, R., Winstead, M., & McEvilley, M. (2022, November 1). *Engineering Trustworthy Secure Systems*. NIST Technical Series Publications. Retrieved September 25, 2023, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf

Sen, K. (2023, June 15). *What is Cybersecurity Risk? A Thorough Definition*. UpGuard. Retrieved October 27, 2023, from https://www.upguard.com/blog/cybersecurity-risk

Spoden, C. (2017, August 22). *Differentiating Between Policies, Standards, Procedures, and Guidelines*. FRSecure. Retrieved December 11, 2023, from https://frsecure.com/blog/differentiating-between-policies-standards-procedures-and-guidelines/

Stine, K., Kissel, R., Barker, W. C., Fahlsing, J., & Gulick, J. (n.d.). *NIST SP 800-60 Volume I Revision 1, Volume I: Guide for Mapping Types of Information and Information Systems to Security Catego*. NIST Technical Series Publications. Retrieved September 28, 2023, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

Stone, M., Irrechukwu, C., & Perper, H. (2018, September). NIST SP 1800-5. *IT Asset Management, A*.

United States of America Department of Commerce. (2004, February). *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*. NIST Technical Series Publications. Retrieved September 25, 2023, from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

What is Unified Endpoint Management (UEM)? (n.d.). IBM. Retrieved December 12, 2023, from https://www.ibm.com/topics/uem