Teppo Kauppinen

Risk and Security Management in SaaS Startup

Metropolia University of Applied Sciences

Master of Engineering

Information Technology

Master's Thesis

03 May 2024

Abstract

Author:	Teppo Kauppinen
Title:	Title of the Thesis
Number of Pages:	55 pages
Date:	03 May 2024
Degree:	Master of Engineering
Degree Programme:	Information Technology
Professional Major:	Networking and Services / Medical Technology
Supervisors:	Ville Jääskeläinen, Principal Lecturer

Startup founders and executives often lack formal training in risk and security management, a key oversight within the fast-paced startup environment. The amount of available information can be overwhelming for anyone without prior domain experience making it impossible to know where to start and what should be prioritised.

This thesis bridges this gap by developing a practical toolkit tailored for cloud-native early-stage startups building SaaS products. The toolkit will focus on core aspects of risk identification, assessment, and mitigation along with cybersecurity best practices for startups.

This thesis is based on the author's work for a Finnish cryptocurrency financing startup in 2021 and 2022 and it has been transformed into generic risk and cybersecurity management guidelines that helps the founders and executives to lead and manage the startup's risk and security.

Keywords: Risk, Cyber security, risk assessment, startup

Contents

List of Abbreviations

2-FA	Two-Factor Authentication. Two-Factor Authentication is an identity and access management security method that requires two forms of identification to access resources and data.
AES-256	Advanced Encryption Standard. Advanced Encryption Standard (AES) 256 is a virtually impenetrable symmetric encryption algorithm that uses a 256-bit key.
AI	Artificial Intelligence.
API	Application Programming Interface. A communication layer for two IT systems to communicate with each other.
AWS	Amazon Web Services. Amazon Web Services, Inc. is a subsidiary of Amazon that provides on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered, pay-as-you-go basis.
B2B	Business-to-business is a business model where a company sells its products or services to other companies.
CCPA	California Consumer Privacy Act. The California Consumer Privacy Act is a state statute intended to enhance privacy rights and consumer protection for residents of the state of California in the United States.
Cloud-Native	Cloud native computing is an approach in software development that utilises cloud computing to "build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds"
CRM	Customer Relationship Management.

CTO	Chief Technology Officer. Typically the highest ranking technology leader of the organisation.
DPO	Data Protection Officer. A data protection officer ensures, in an independent manner, that an organisation applies the laws protecting individuals' personal data.
EU	European Union.
FIVA	Finanssivalvonta - Finnish Financial Supervisory Authority.
GCP	Google Cloud Platform. Google Cloud Platform is a suite of cloud computing services that provides a series of modular cloud services including computing, data storage, data analytics, and machine learning, alongside a set of management tools.
GDPR	General Data Protection Regulation is a European Union regulation on information privacy in the European Union and the European Economic Area.
GKE	Google Kubernetes Engine. A fully managed Kubernetes as a service in Google Cloud Platform (GCP).
IT	Information Technology.
KYC	Know Your Customers. A mandatory process in certain business areas (e.g. financing, investment) of identifying and verifying the client's identity.
NIST	The National Institute of Standards and Technology is an agency of the United States Department of Commerce whose mission is to promote American innovation and industrial competitiveness.

PII	Personally Identifiable Information. Personally Identifiable Information or Person Data is any information related to an identifiable person.
SaaS	Software as a Service (SaaS) is a cloud-based software delivery model where applications are hosted by the vendor and accessed by customers over the internet, typically on a subscription basis.
SfSD	Startups for Sustainable Development is a startup program by Google for sustainability focused startups.
SQL	Structured Query Language. Structured Query Language is a language used to manage data, especially in relational database management systems.
SSL	Secure Sockets Layer. A security protocol that creates an encrypted link between two IT systems.
VP	Vice President. Vice President is an organisational leadership role.
TLS	Transport Layer Security. TLS is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet.
UI	User Interface.

1 Introduction

Startup companies are typically focused on building a new product as fast as possible to get access to users, to start generating revenue, and to validate product-market fit. Founders of startups, often domain experts in areas such as marketing, sales, or technology, frequently lack risk and security management experience. While this absence of risk and security proficiency may not pose an immediate issue at the beginning of the journey, its importance grows when the product or service is launched, the user base expands, and the need for (additional) funding arises.

Risk and security management is a broad topic and typically focuses on well-established companies that have the required resources to set up the recommended policies and processes. This is more challenging in startups where business, marketing and product goals compete for the extremely limited resources. It is hard to justify prioritising risk and security when you don’t have a working product, any customers or revenue.

Additionally, the overwhelming amount of information online makes it hard for the founders to know where to start and what to prioritise and the available certifications can take years to achieve. As a result, risk and security management is often overlooked in these companies which can lead to significant problems in the future.

This master's thesis examines risk and security management within the product and operations lifecycle of early-stage cloud-native SaaS startups. Other risks (such as organisational, investment, physical) are not considered, although the same approach (identify-analyse-assess-document-mitigate) can be used for those.

The goal of this master's thesis is to create a practical risk and security management handbook for startup founders and executives without prior experience. The handbook will provide understanding of the key aspects of risk and security management, the key focus areas, and how to get started. As risk and security management is such a broad topic and varies from business to business, it is impossible to provide a definite guidance. Instead, the goal is to provide a bare minimum framework that allows the startups to get started with the risk and security management and that can be expanded to meet later needs while the business grows. Additionally, the goal is to enable non-technical stakeholders to continuously manage risk and security aspects as part of the daily operations.

The thesis is based on cybersecurity frameworks such as NIST and the author's Cyber Security Specialisation Studies, his risk and security management work in a Finnish startup company, and his work as a startup advisor at Google, where the author has advised multiple startups on how to manage risk and security in early-stage startup companies.

This thesis has been divided into 5 sections. The first section introduces the problem and the second section provides background information. The third section introduces what risk and security management is. The fourth section proposes a lightweight risk and security management framework for SaaS startups and the last section summarises the findings and provides a high level diagram of the framework.

2 Background

Tesseract Investment is a Finland based Finnish Financial Supervisory Authority (FIVA) regulated startup that provides financial services to cryptocurrency markets. The company raised a 25M€ investment to enable growth and international market expansion, to expand their product portfolio, and to develop modern API based financial services to B2B cryptocurrency markets. To achieve these goals, the company must be able to build partnerships and provide services to key players in the cryptocurrency markets.

Financial markets are based on trust and the key quality of any company is trustworthiness. The partners and customers must be able to trust that their financial assets are well managed and they are able to get their financial assets back. A company that cannot be trusted for example due to its financial situation, lack of domain expertise, or poorly managed operations is quickly out of business. [1]

When the total yearly financial transactions between the companies can be in the hundreds of millions and beyond, the companies must be able to demonstrate trustworthiness and business continuity even in the case of an emergency such as data loss, ransomware, or hacking related incidents. Risk and security management plays a crucial role when demonstrating trustworthiness.

Tesseract Investment already had a solid financial situation and strong domain expertise and it was time to set up a structured risk and security management framework that will support the company's growth.

As an advisor in Google's Startups for Sustainable Development (SfSD) program, the author of this master's thesis has advised 30+ startups regarding multiple topics. A few of the startups have requested advisory sessions regarding risk and security management where the author has helped the

startup founders and key technical stakeholders to understand and gain insights on how to approach the topic in their company.

The groundwork for this thesis was done at Tesseract Investment and as part of the SfSD program. The company specific parts have been excluded and instead the focus is on the common parts of the mentioned work with the goal of creating a lightweight risk and security management framework for early stage SaaS-startups that operates using public cloud (Amazon AWS, Google Cloud, Microsoft Azure).

3 Risk and Security Management

This section describes the key aspects of risk and security management. It starts with a simple example and two AI made definitions of Risk and Security Management.

Consider the following example

> Company A and Company Z experience similar data losses. However, Company Z demonstrates transparency by providing documentation of their mitigation strategies, backup strategy, analysis of the incident, and how they plan to improve their approach. Company A provides no such details. Whose service would you be more likely to continue using?

The simple example above highlights the importance of risk and security management, which is defined by Google Gemini Advanced AI below:

> “Risk and security management is the ongoing process of identifying potential threats and vulnerabilities to an organisation, assessing the likelihood and potential impact of those risks, and implementing proactive measures to reduce or eliminate them. This includes safeguarding an organisation's physical and digital assets, ensuring compliance with laws and regulations, and building resilience against disruptions that could harm the business's reputation, operations, or financial stability.” - Google Gemini AI Advanced when asked to define risk and security management.

When asked to define risk and security management in early-stage startup companies, Gemini produced the following answer:

> “Risk and security management in an early-stage startup company involves proactively identifying and addressing the unique threats and vulnerabilities the business faces as it rapidly grows and evolves. This means recognizing potential risks to the company's finances, operations, intellectual property, and reputation, then taking calculated steps to minimise those risks before they cause major damage. Founders must actively protect their assets, customer data, and the trust of early investors, all while operating within limited resources and a fast-paced, often unpredictable environment.”

In other words, risk and security management is a structured and systematic approach of identifying, analysing, assessing, documenting, and mitigating the risks. [2][7]

Risk management focuses on broad identification, analysis, and mitigation of all potential risks that could have an impact on an organisation's goals, assets, operations, and reputation. This includes, but is not limited to [1]

- **Financial risks** such as failing to raise funding, losing a major customer, or unpaid invoices by customers.
- **Operational risks** such as supply chain problems, key personnel leaving the company, database crash, and payment system failures.
- **Strategic risks** such as a well-known tech giant adding similar products to their portfolio or buying a direct competitor.
- **Intellectual Property risks** such as failing to file a patent successfully or using patented technology as part of the company’s products and services.
- **Legal risks** that arise when the laws and regulations change. For example, GDPR was a huge risk for any company that based its business on collecting and sharing personal information (like social media).
- **Reputational risks** such as negative publicity and scandals that are often byproducts of other risks.

(Information) Security management is a subset of risk management with a focus on security threats and risks. Security management can further be divided into smaller domains including at least [6]

- **Cybersecurity** protects the IT systems and networks.
- **Data Security** protects the confidentiality, integrity and availability of all the data the company owns.
- **Endpoint Security** safeguards physical hardware such as mobile phones and laptops.
- **Access Controls** safeguards access to data and systems preventing unauthorised access.
- **Physical security** safeguards access to offices or any other physical premises the company has.

The company specific risk and security management approach varies based on the organisation’s size and industry and the related legal requirements. Also, it’s good to understand that the risks and technical threats are always company specific as those are based on the company’s offering (product/service), technology stack, partners, third-party providers, and so forth. [3]

Risk and security management must be included into the daily operations of the company. For example, when the company forms a partnership or starts using a third-party service/product, the company should document the risks and the related mitigation strategies. The process should be lightweight to reduce any unnecessary overhead and mandatory to make sure the documentation is always up to date.

The key aspects of risk and security management are **policies**, **documentation**, **processes**, and **progress tracking**.

Policies

Policies are formal documents and standards that define the startup’s approach to risk and security management. The policies are required to establish clear guidelines, expectations, and standards for protecting an organisation's assets, operations, and reputation from potential risks and security threats. After definition, the policies should guide all later work to ensure it meets the requirements.

For example, in data retention policy, the company can define that the maximum amount of data (in time) that can be lost in any incident is 4 hours. This requirement sets the expectations for database backups and technical operations as those must be planned accordingly to meet the 4-hour requirement.

Documentation

Documentation provides an overview of the current state of risk and security management. It provides both a roadmap and a historical record of identified

risks, their likelihood, severity, business impact, and mitigation strategies. The documentation increases transparency within the company and strengthens the startup's ability to manage risk and security in a controlled manner.

Additionally, in the case of a cyber attack, documentation works as an evidence that the company adhered to industry best practices and proactively implemented measures to mitigate identified risks. By being able to prove the startup adhered the industry best practices, it is possible to reduce the amount of financial and reputational losses.

Tracking Progress

When any work has been identified, it should be tracked to ensure the work will be delivered in a timely manner. The tracking can be done using common tools such as project management tools or issue tracking software. The selected tool should provide details of each work item, who are the owners and what is the status of the work items. The owners should also keep the work items updated by including relevant information such as links to updated documentations for verification purposes.

For example, when the startup integrates its SaaS product to a third-party payment provider, it should add new work items e.g. to update the architecture documentation, service catalogue, and disaster recovery plan. It should also add tasks to perform risk assessment and business impact analysis, and to update business continuity plan. The tools also provide historical data of work items. For example, if there is a need to know who set up the automated database backups and when, the tool can be used to find the related task that holds the relevant information.

Process

Risk and especially security domains are often considered by many as technical hands-on work. While the actual mitigation work is often both hands-on and technical, managing risk and security is neither, and the mitigation is often the last step of the process. Instead, like defined by Gemini, risk and security

management is a continuous process of **identifying**, **analysing**, **assessing**, **documenting**, **mitigating the risks**, and **tracking the progress**. [2]

A simplified example of identifying, analysing, assessing, and mitigating the risk could be as follows

- **Identify risk:** EU GDPR compliance
- **Analyse:** EU GDPR regulation protects all EU citizens and their personal information regardless of where the company is located or operated, or where the data is stored.
- **Assess:**
    - Risk probability: medium
    - Severity: high
    - Impact
        - up to 10M€ or 2% of global turnover, whichever is higher.
        - Loss of reputation
        - Loss of business
- **Mitigation:** Restrict internal access to user data, restrict user data shared to third-parties, only use GDPR compliant third-party service providers, keep data processing records up-to-date, allow users to withdraw consent, allow users to be forgotten (deletion of data), enable/allow users to request/access personal data.

An example of a technical risk could be as follows

- **Identify risk:** Database is unavailable.
- **Analyse:** Company Y provides database-as-a-service and automatic database backups. Company Y can have long running technical issues, company Y can get hacked, declare bankruptcy, or refuse to offer services to Our Company.
- **Assess:**
    - Risk probability: low
    - Severity: high
    - Impact:
        - Service is unavailable for users

        - Loss of data and backups
        - Loss of reputation
        - Loss of business
    - **Mitigation:** Have backups available in alternative location, select secondary service provider, create required accounts to secondary service provider, software architecture must support switching database service provider, document and test backup restoration to secondary service provider.

After the risks have been identified and assessed, and the mitigation strategies have been decided, the documentation should be updated and the related work should be tracked using a tool.

Most of this work, with the exception of some mitigation activities, requires only tools that most companies already have like an office suite (Microsoft Office or Google Workspace) or any comparable documentation tool such as Wiki.

4 Managing Risk and Security in Early-Stage SaaS-Startup

Managing risk and security follows the same principles regardless of the size of the company. One main difference between a well established company and an early-stage startup is the amount of available resources. Fortunately the startups are also exposed to a limited amount of risks due to the size of their business and limited complexity of their technical systems. This allows the startups to manage their risks and security as long as they know where to focus.

Each startup has a unique set of risks and security threats, legal and regulatory requirements, and so forth. As such, it is only possible to provide a baseline that can be extended when the startup gains more experience, and the business grows exposing new risks and threats.

The following sections introduce a baseline for risk and security management policies and documents. This section does not provide highly detailed information as the suggested policies and documentation are well documented online. Instead, the goal is to provide enough information to understand why each policy and document is required and how it helps to manage risk and security.

To showcase a simple process that can be used to integrate risk and security management into the daily operations of the company, the following example will be used

> Company is building a SaaS service and the company must Know Your Customers (KYC) meaning they must identify and verify their customers identities when a new user account is created. The identity verification must be based on government issued identity cards and the company decides to use a third-party service provider that provides such service. This means the company must do a technical integration and provide user data to the third-party service provider.

The following sections contain items in black and red colour

- The items with black colour represent the previous state without the identity verification requirement.
- The items with red colour represent newly added components, identified risks, and so forth that are needed for the identity verification feature.

4.1 Baseline Documentation

To start managing risk and security of their SaaS-service, the startup should first create a baseline documentation that provides a high level understanding of the system and its components.

- **Architecture Documentation:** Provides overview of the system, its components, third-party services, and the related data flows.
- **Service Catalogue:** Service catalogue provides overview of all the services, technologies, dependencies, and subscriptions of the company.

These documents work as a reference documentation that will help greatly when managing risk and security and creating the required policies and other documents.

4.1.1 Architecture Documentation

Architecture documentation provides a clear and concise overview of the used technology stack, system's components and the data flows between the components. The documentation should be concise and flexible and focus on creating a shared understanding of the system's core components and how they interact. This includes a high-level diagram outlining components like the front-end, back-end, databases, and any external services.

One of the most important parts of the architecture documentation is the architecture diagram that provides an overview of the system, its components, used third-party services, and related data flows.

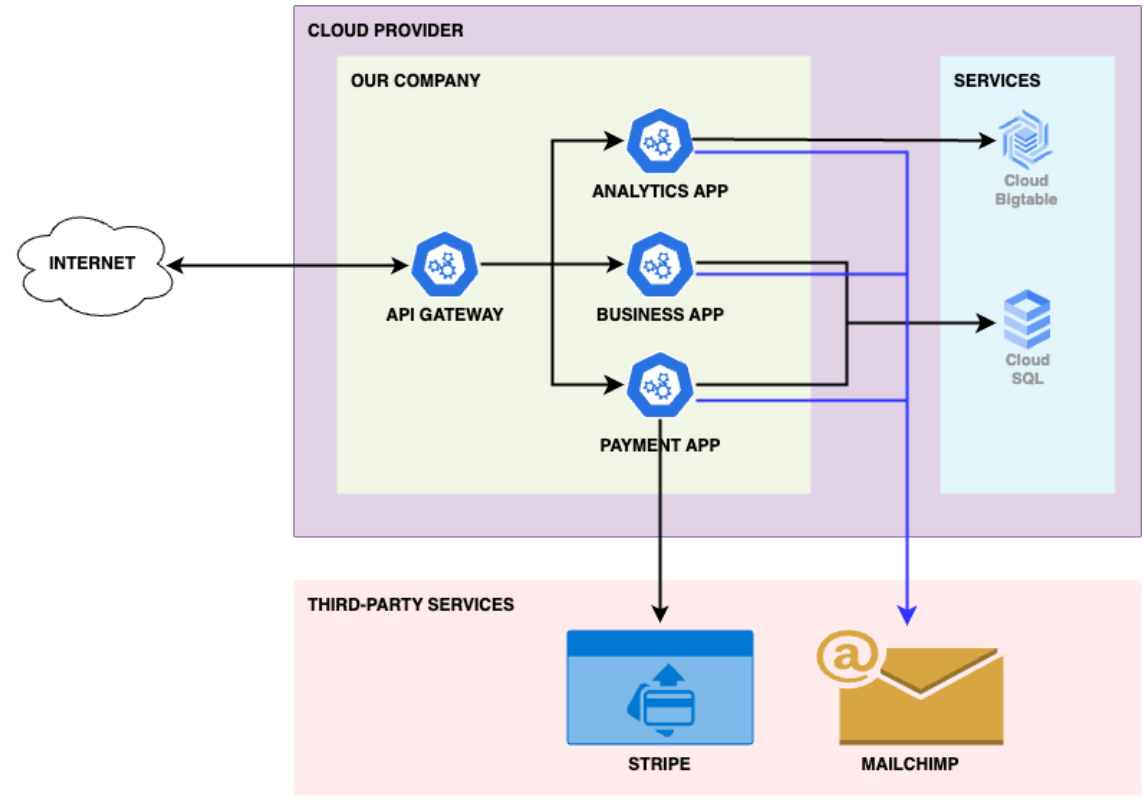

Figure 1. A simplified Architecture Diagram.

The Identity App, Identity Verifier, and CloudSQL are new components that are required to fulfil the identity verification requirement.

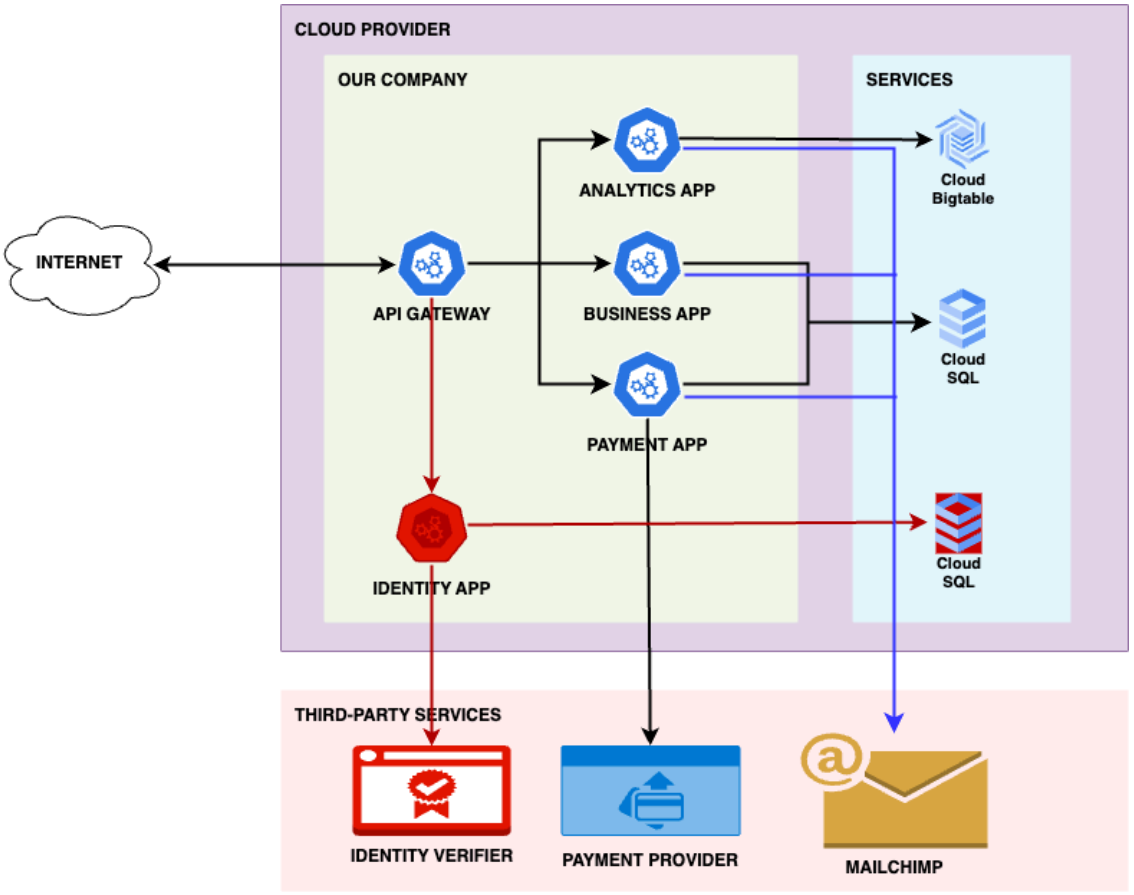

Figure 2. A simplified Architecture Diagram.

More information about Architecture Documentation can be found in reference [8].

4.1.2 Service Catalogue

Service Catalogue lists all services and technologies the company owns, develops, or uses including internal and external services such as databases, cloud services, CRM systems, marketing and communication tools. Service catalogue provides an easy to understand overview of all the used services, who provides the services, what is the purpose of the service, and who owns the service internally. Service catalogue also enables tracking and estimating costs by adding the service specific costs to it.

Architecture documentation is a good starting point when creating the service catalogue as it provides an overview of the system and its dependencies.

Table 1. A simplified Service Catalog.

Provider	Service	Use	Date	Owner	Cost
Google	Cloud	Cloud Platform	01.01.2024	CTO	0€ per month
Google	Cloud SQL	Database	01.02.2024	CTO	80€ per month
Google	Cloud Bigtable	Data Analytics	01.02.2024	Head of Analytics	200€ per month
Google	GKE	Container orchestration, production and test environments.	01.02.2024	CTO	240€ per month
Stripe	Payment Provider	Credit card payments	01.03.2024	CTO	20€ per month + 2.5% per transaction
GoDaddy		Domain Registration	01.02.2024	CEO	20€ / 3 years
Slack	Chat	Chat	01.01.2024	COO	10€ per employee
Google	Workspace	Email, Office tools	01.01.2024	CEO	12€ per employee
Idenfy	Identity Verification	Identity Verification	01.03.2024	CTO	2€ per verification

More details of a service catalogue can be found in reference [9].

4.2 Policies

Policies are formal documents and standards that define the startup’s approach to risk and security management. The policies are required to establish clear guidelines, expectations, and standards for protecting an organisation's assets, operations, and reputation from potential risks and security threats. After definition, the policies should guide all later work to ensure it meets the requirements of the defined policies.

Customer data is one of the most valuable assets of any company. If the data is lost or leaked, or if it is accessed without authorization, the company can face serious consequences such as fines, loss of reputation, or bankruptcy. This is especially true for a SaaS startup where loss of reputation easily leads to bankruptcy.

To protect its customer data, the startup should define clear policies of how the data is managed and accessed within the company. The following policies can be considered as a baseline for protecting the customer data: [33][34][35]

- **Password Policy**: Password policy defines (minimum) requirements for all passwords.
- **Data Retention Policy:** A data retention policy outlines the guidelines for how long the company stores data, including the purposes for storage and procedures for secure disposal when the retention period ends.
- **User Data Access Policy:** A user data access policy defines the rules and permissions that govern who can access what user data within an organisation's systems, and under what circumstances, ensuring data privacy and security.
- **Encryption Policy:** An encryption policy defines the standards, procedures, and technologies an organisation uses to encrypt sensitive data both at rest and in transit, ensuring its confidentiality and protection from unauthorised access.

- **Secrets Management Policy:** A secrets management policy defines the secure procedures for storing, accessing, rotating, and auditing sensitive credentials (such as API keys, passwords, and certificates) used within an organisation's systems and applications.

The policies contribute not only to both risk and security management, but also towards the company's privacy management efforts as it defines where the user data is stored and how and why it can be accessed.

4.2.1 Password Policy

A password policy sets the (minimum) requirements for any password used by an employee, user, or customer. The goal is to reduce the risk of unauthorised access due to weak or compromised passwords. The password policy can contain different requirements for different systems; for example, password requirements for the administrative UI of the SaaS-service might be significantly stricter than requirements for the user/customer passwords.

Requiring users and customers to use strong passwords and optionally using two-factor authentication reduces the risk of customer account hijacking and/or data leak. While the startup may not be directly responsible for the weak passwords or the possible consequences (account hijacking, data leak), it can still cause significant loss of reputation and loss of revenue for the company when customers or potential new customers learn about it.

Table 2. A simplified Password Policy.

TYPE	LENGTH	COMPLEXITY	PROHIBITED	2-FA REQUIRED	EXPIRATION
Internal employee password	16	Uppercase and lowercase letters, numbers,	First name, last name, sequential numbers,	YES	365 days

		special characters	email address		
Administrative UI password for employees	16	Uppercase and lowercase letters, numbers, special characters	First name, last name, sequential numbers, email address	YES	90 days
Customer password for SaaS service	10	Uppercase and lowercase letters, numbers, special characters	Name, sequential numbers, company name, email	NO	365 days

More information about password policies can be found in reference [10].

4.2.2 Data Retention Policy

A data retention policy outlines the guidelines for how long the company stores data, including the purposes for storage and procedures for secure disposal when the retention period ends. A data retention policy guides the technical implementation of storing the data and the related backups. It also addresses legal requirements and privacy obligations. For example, financial companies may have a requirement to store all data for 10 years whereas for other businesses storing all data for 10 years might be problematic from the GDPR perspective.

The data retention policy should include details of [11]

- how different types of data are being stored.
- why it is being stored.
- where it is being stored.
- how long the data is being stored.
- how the stored data is being protected (encryption, other methods).
- how the data will be cleaned after the retention period ends.

Table 3. A simplified Data Retention Policy.

Category	Storage Location	Retention Period	Justification	Security Measures	Disposal Method	Owner
Payment Data	Database	10 years	Required by law	Encrypted at rest, Encrypted in-transit		CFO
Customer Data	Database	forever	Data added by customers who expect it to be available forever.	Encrypted at rest, Encrypted in-transit	Manual deletion by the customers	CTO
Payment Data	Cloud BigTable	3 years	Financial analytics	Encrypted in-transit		CFO
Usage Data	Cloud BigTable	1 year	Usage analytics to improve our service	Encrypted in-transit		Head of Analytics
Database Backups	Cloud storage	Daily backup: 30 days Weekly backup: 1 year Monthly backup: 10 years		Encrypted at rest, Encrypted in-transit	Automatically by cloud storage	CTO
Logs	Cloud Logging	30 days	Security, Operational, Debugging	Encrypted in-transit	Automatic	CTO
Logs	Cloud storage	2 years	Long term storage of logs for security and debugging purposes.	Encrypted at rest, Encrypted in-transit	Automatically by cloud storage	CTO
Identity Verification Data	CloudSQL	forever	KYC requirement	Encrypted at rest, Encrypted in-transit		CTO
Identity Verification Data	Idenfy	forever	KYC requirement	Encrypted at rest, Encrypted in-transit		CTO

More information about data retention policies can be found in reference [11].

4.2.3 User Data Access Policy

Many SaaS services store significant amounts of user data. This can be the users' personal information such as name, address, credit card information or, for example, data that the users have added or imported to the service. Access to certain data such as personal, financial, or health information may be protected by laws and regulations, but it's recommended that access to all user data is protected and allowed only with a proper justification.

As an example of the importance of User Data Access Policy, consider the following example

> You have purchased your groceries from an online retailer for some time. Would you like that every software developer or customer service specialist from the online retailer have access to your order history? What if it was your identity information that can be used for identity theft?

A user data access policy defines who has permission to access various types of user data, for what purposes they can use it, and under what conditions or circumstances access will be granted. This policy is designed to protect the privacy and security of user data by ensuring that access is limited to those with legitimate need, that usage aligns with specified purposes, and that appropriate safeguards are in place to prevent unauthorised access or misuse. The user data access policy also sets technical requirements for the company's SaaS service and other systems as those have to be able to adhere to the policy.

Table 4. A simplified User Data Access Policy.

CATEGORY	ACCESS	USE CASES	REQUIREMENTS
Customer Personally Identifiable Information (PII)	Customer Support team	Limited access to first name, last name, email, phone number for customer support purposes.	1. Formal training on data security and privacy for all authorised personnel. 2. Multi-factor authentication. 3. Role-based access control 4. Customer support id included in the

			audit logs
Customer Personally Identifiable Information (PII)	Marketing team	Limited access to first name, last name, birthday, email address and communication preferences for marketing purposes.	1. Formal training on data security and privacy for all authorised personnel. 2. Multi-factor authentication. 3. Role-based access control
Customer Personally Identifiable Information (PII)	Engineering team	Full access for resolving related technical issues.	1. Formal training on data security and privacy for all authorised personnel. 2. Multi-factor authentication. 3. Role-based access control 4. Bug id included in the audit logs
Customer Billing Information	Customer Support	Limited access for troubleshooting payment issues.	1. Formal training on data security and privacy for all authorised personnel. 2. Multi-factor authentication. 3. Role-based access control 4. Customer support id included in the audit logs
Customer Billing Information	Financial Operations	Full access for processing financial transactions, account management, and reporting.	1. Formal training on data security and privacy for all authorised personnel. 2. Multi-factor authentication 3. Role-based access control 4. Access is logged
Customer Billing Information	Engineering team	Full access for resolving related technical issues.	1. Formal training on data security and privacy for all authorised personnel. 2. Multi-factor authentication. 3. Role-based access control 4. Bug id included in

			the audit logs
Identity Verification Information	Director Of Engineering, Lead Developers.	Full access for resolving related technical issues.	1. Formal training on data security and privacy for all authorised personnel. 2. Multi-factor authentication. 3. Role-based access control 4. Bug id included in the audit logs
Identity Verification Information	Legal Operations	To fulfil legal and regulatory requirements.	1. Formal training on data security and privacy for all authorised personnel. 2. Multi-factor authentication. 3. Role-based access control

More information about User Data Access Policy can be found in references [12][13].

4.2.4 Secrets Management Policy

A secrets management policy defines the secure procedures for storing, accessing, rotating, and auditing sensitive credentials (such as API keys, passwords, encryption keys, and certificates) used within an organisation's systems and third-party services.

The importance of the secrets management policy can be highlighted with a simple example

> A startup has a team of 20 engineers and over the recent years 10 engineers have left the company. The startup has been using a shared password manager KeePass for storing API keys, passwords, and certificates. This means 10 former employees can still have access to the company’s highly confidential API keys, passwords, and certificates - and the startup has very limited options for verifying this or if the secrets have been used for unauthorised access, may it be by the current or former employees.

The secrets management policy addresses the issue by providing guidelines on [15]

- How the secrets shall be stored?
- Who can access the secrets?
- How can secrets be accessed?
- What are valid business reasons for accessing the secrets?
- How is access to the secrets monitored and audited?
- How often the secrets are rotated (meaning how often new secrets, that will replace the previous secrets, are generated)?
- How are the keys rotated?

The previously introduced documents - architecture documentation, architecture diagram, service catalogue, and data retention policy - provides the necessary details for creating the secrets management policy.

Secrets Management Policy

Purpose

This policy establishes secure procedures for storing, accessing, rotating, and auditing sensitive credentials (API keys, database passwords, certificates, etc.) used within our SaaS development and operations environments.

Scope

This policy applies to all employees, contractors, and automated systems that interact with secrets.

Policy Statements

What Are Secrets

- Secrets include but are not limited to:
  - API Keys and tokens
  - Database and system passwords
  - Encryption keys
  - TLS/SSL certificates
- Secrets Storage
  - Secrets MUST NOT be stored in plain text in code, config files, or spreadsheets.
  - Secrets will be stored in a centralised secrets management system
  - Only authorised personnel will have access to the secrets

management system.
        - Authorised personnel include the company's technological leadership (CTO, VP, Director) and lead developers.
- Secrets Access
    - Access to secrets will follow the principle of least privilege.
    - Applications and scripts will retrieve secrets at runtime using secure APIs or environment variables provided by the secrets management system.
    - Manual access will be logged and require justification.
- Secrets Rotation
    - A schedule for rotating secrets will be defined based on risk and ease of rotation.
        - Database secrets: every 3 months
        - API keys: every 6 months
        - TLS/SSL certificates: monthly
        - Encryption keys: monthly
    - Critical secrets (e.g., database master passwords) will require immediate rotation upon compromise or unauthorised access.
- Incident Response
    - Suspected compromise of secrets will be reported immediately and treated as a potential security incident.
    - Incident response procedures will include steps for revoking and rotating affected secrets.

More information about secrets management policy can be found in references [14][15].

4.2.4 Encryption Policy

An encryption policy defines the standards, procedures, and technologies an organisation uses to encrypt sensitive data both **at rest** (when the data is stored to a storage system, including databases) and **in transit** (when the data is transferred between different components or systems), ensuring its confidentiality and protection from unauthorised access.

Encryption Policy

Purpose

This policy outlines the standards for using encryption to protect the confidentiality and integrity of sensitive customer data and company information within our SaaS platform.

Scope

This policy applies to all employees, contractors, and third-parties with access to [Company Name] systems and data.

Policy Statements

- Data Classification
  - All data will be classified according to a Data Classification Policy (Confidential, Internal, Public).
  - Confidential data (e.g., customer PII, financial records, intellectual property) MUST be encrypted at rest and in transit.
- Encryption Standards
  - Encryption at rest will use at minimum AES-256.
  - Encryption in transit will use TLS 1.2 or higher.
  - Approved encryption algorithms may be updated as technology and best practices evolve.
- Key Management
  - Encryption keys will be stored in a secure key management system.
  - Access to encryption keys will be on a need-to-know basis and logged.
  - A key rotation process will be defined.
- Vendor Requirements
  - Vendors handling Confidential data must employ encryption standards equivalent to or exceeding those outlined in this policy.

Responsibilities

- Development Team: Responsible for implementing encryption according to these standards.
- Security Officer: Responsible for policy maintenance and reviewing encryption controls.
- All Employees: Responsible for reporting suspected breaches or policy violations.

More information about encryption policies can be found in references [16][17].

4.3 Managing Risk

Risk management in an early-stage SaaS startup is to proactively identify, assess, and prioritise potential risks that could disrupt operations, damage the company's reputation, threaten the customer data, or prevent it from achieving its goals. By systematically considering internal and external threats, a company can develop strategies to avoid, mitigate, or transfer risk, minimising their

negative impact and increasing the chances of survival and success in the long run.

The following processes/documentations can be used as a starting point [37][43]:

- **Risk Assessment:** Risk assessment provides overview of identified risks, their business impact, likelihood and severity, and chosen mitigation strategies.
- **Business Impact Analysis:** A business impact analysis (BIA) is a process that identifies critical business functions, analyses the potential consequences of their disruption, and helps prioritise recovery efforts based on their impact on the organisation. Business Impact Analysis is typically part of the Business Continuity Plan.
- **Business Continuity Plan:** A business continuity plan (BCP) is a detailed strategy for how an organisation will maintain critical operations, minimise disruptions, and recover quickly in the event of a disaster or major incident.
- **Disaster Recovery Plan:** A disaster recovery plan is a documented set of procedures designed to restore critical IT systems, data, and operations in the aftermath of a disruptive event (natural disaster, cyberattack, etc.), minimising downtime and ensuring business continuity.
- **Incident Management Process**: An incident management process is a structured approach to responding to incidents.

Business impact analysis is a critical part of the business continuity plan. Additionally, the business impact analysis and the risk assessment are closely related.

- **Risk Assessment**: Focus on identifying and evaluating the possible disruptions.
- **Business Impact Analysis (BIA)**: Focus on what are the business consequences of a possible disruption.

- **Business Continuity Plan (BCP)**: Focus on how to continue operations during and after disruption.

In other words, **Risk Assessment** provides details on what could go wrong and how likely it is, **Business Impact Analysis** provides details on business impacts of the possible disruptions, and **The Business Continuity Plan** provides details on how to recover and maintain operations during the disruptions. Additionally, the **Disaster Recovery Plan** allows the startup to restore its SaaS-service into functional state.

4.3.1 Risk Assessment

Risk assessment is used to identify potential threats that could cause issues to product development, harm customer data, disrupt service delivery, or damage the company's reputation. By systematically analysing risks related to technology, security, operations, finances, and compliance, startups can develop strategies to mitigate those risks, prioritise protective measures, and make informed decisions that safeguard the business's success and its customers' trust.

Risk assessment can be performed using a simple spreadsheet (Microsoft Excel, Google Sheets) or table in a documentation tool. Each entry contains details of the risk and its probable causes, possible impact(s) of the risk and how to mitigate it. Each entry also contains a calculated risk priority number (RPN), which can be used to prioritise the mitigation efforts. The higher the RPN, the higher the priority of the mitigation. RPN is calculated as follows [38]

- **Frequency:** On the scale of 1 (rarely) - 5 (very often), how often the risk occurs / how likely is the risk?
- **Severity:** On the scale of 1 (negligible) - 5 (huge), how severe is the impact of the risk?
- **Detectability:** On the scale of 1 (easy) - 5 (very hard), how easy is it to detect the risk?
- **RPN = Frequency x Severity x Detectability**

Table 5. A simplified Risk Assessment.

RISK	CAUSE	IMPACT	MITIGATION	FREQUENCY	SEVERITY	DETECTABILITY	SCORE (RPN)
Google Cloud permanently unavailable	Breach of contract, unpaid bills, international sanctions.	Service unavailable	Document options for transferring services to alternative cloud platforms.	1	5	1	5
Payment provider is unavailable permanently or for a long period of time.	Payment provider bankruptcy, Payment provider hacked, Payment provider declines to provide the service to Our Company, Our company can't use Payment Provider for legal reasons (sanctions)	Payments cannot be processed, loss of revenue, customers cannot purchase or upgrade subscription, customers cannot access paid features.	Verify payment provider's financial status, technical competency, relevant certifications. Pre-select a secondary payment provider, create required accounts, technical integration, test technical integration, document how to switch from primary to secondary provider.	1	3	1	3
Payment Provider data leak	Payment provider is hacked or accidentally leaks the confidential data	Confidential customer data is leaked. Loss of reputation that can lead to loss of business.	Verify Payment Provider has industry standard security certifications.	1	2	3	6
Identity Verification Provider unavailable	Technical problems, ransomware, bankruptcy	New customers cannot register.	Verify identity verification provider's financial status, technical competency, pre-select a secondary identity verification provider.	1	2	1	2

Identity Verification Provider data leak	Payment provider is hacked or accidentally leaks the confidential data	Confidential customer data is leaked. Customers may face identity theft. Loss of reputation.	Verify Payment Provider has industry standard security certifications.	1	5	5	25

When performing a risk assessment, the focus should be on risks that require (somewhat) immediate action to reduce the amount of identified risk and unnecessary work. For example, the cloud platform could decide to deprecate a service that Our Company is using. Even if this exposes a risk to Our Company, there is typically a relatively long period of time between the announcement of the deprecation and the day when the service will be shutdown. This leaves Our company enough time to react to the announcement and create a mitigation plan.

More information about risk assessments can be found in reference [18][36].

4.3.2 Business Impact Analysis

A Business Impact Analysis (BIA) is a process that identifies an organisation's critical functions and processes, analyses the potential consequences (financial, operational, reputational) if they were disrupted, and prioritises their recovery efforts based on the severity of the impact. The BIA serves as the foundation for developing a business continuity plan by outlining what needs to be protected most urgently and informing decisions about resource allocation and resilience strategies.

Business impact analysis is a high level document that focuses on identifying critical business functions and processes and their impact on business in the case of disruption.

Table 6. A simplified Business Impact Analysis.

EVENT	REASON	OUTCOME	IMPACT	RTO
Google Cloud temporarily unavailable	Major issues in Google Cloud infrastructure	Service completely unavailable to customers	1. Revenue: 100-125€ per hour 2. Loss of reputation	-
Database unreachable	Major issues in Google Cloud infrastructure, accidental deletion of the database, database crash	Service completely unavailable to customers	1. Revenue: 100-125€ per hour 2. Loss of reputation	4h
Data loss in Cloud BigTable	accidental deletion of data, bug in the code	Analytics features not working properly for some or all of the customers	1. Loss of reputation	4h
Data loss in Cloud SQL	Database crash, accidental deletion of data, bug in the code, hackers, ransomware,	Payment and business features of the service are not working properly to some or all of the customers	1. Revenue 100-125€ per hour 2. Loss of reputation 3. Possible discounts from future subscription fees	4h
Payment Provider temporarily unavailable	Issues in payment provider infrastructure, Issues in technical integration, unpaid bills	New customers cannot purchase paid subscriptions. Existing customers cannot renew or upgrade subscriptions. Paid features not available to new customers or customers willing to upgrade subscription.	1. Revenue: 300€ per day	12h
Payment Provider permanently unavailable	Payment provider bankruptcy, payment provider refuses to serve Our	New customers cannot purchase paid subscriptions. Existing customers	1. Revenue: 300€ per day	48h

	Company.	cannot renew or upgrade subscriptions. Paid features not available to new customers or customers willing to upgrade subscription.		
Identity Verification Provider temporarily unavailable	Issues in provider infrastructure, issues in technical integration, unpaid bills	New customers cannot register.	1. Revenue: 300€ per day	12h
Identity Verification Provider permanently unavailable	bankruptcy, payment provider refuses to serve Our Company.	New customers cannot register.	1. Revenue: 300€ per day	48h

More information about Business Impact Analysis can be found in references [19][20].

4.3.3 Business Continuity Plan

Even if an organisation's risks are well managed, sometimes unexpected events such as fire or a cyber attack can cause disruptions to operations and it is crucial for any business to be able to continue its operations as soon and smoothly as possible.

A business continuity plan (BCP) is a comprehensive strategy that outlines how an organisation will maintain critical operations, minimise disruptions, and recover as quickly as possible in the event of a disaster or major incident. It includes identifying essential business functions and assessing potential risks, and developing procedures to respond and recover from disruptions.

In addition to the previously introduced **Business Impact Analysis** and **Risk Assessment**, the **Business Continuity Plan** should cover at least two new topics [21][42][43]

- **Recovery Strategies:** Defines how to recover from different types of disruptions.
- **Incident Response Plan:** Defines procedures and chain of command for immediate response to disruption.

More information about the Business Continuity Plan can be found in references [21][22][23].

Recovery Strategies

The Recovery Strategies defines how to recover from different types of disruptions identified during the risk assessment. Each strategy should contain detailed instructions to restore a fully functioning state and to resume the operations.

For example, to recover the company's SaaS service after a cyber attack that led to loss of data, the disaster recovery plan should be used as it provides the required instructions to fully recover the system to functional state.

Table 7. A simplified Risk Assessment.

RISK	CAUSE	IMPACT	MITIGATION
Payment provider permanently unavailable	Payment provider bankruptcy	Payments cannot be processed, loss of revenue, customers cannot purchase or upgrade subscription, customers cannot access paid features.	Verify current payment provider's financial status, Select a secondary payment provider, migrate to secondary payment provider.
Identity Verification Provider permanently unavailable	Identity Verification Provider bankruptcy, Identity Verification Provider refuses to serve Our Company	New customers cannot register.	Verify current provider's financial status, Select a secondary provider, migrate to the secondary provider.

The high-level recovery strategy for the “payment provider permanently unavailable” risk could be as follows

- Temporarily allow all customers to access paid features.
- Migrate to another payment provider.
- Restrict access to paid features.

This recovery strategy would allow all customers to use the service with a minimal disruption without any **additional** loss of revenue to Our Company (there is no revenue during the incident as the payments cannot be processed). To limit the length of the disruption, to minimise financial losses, and to ensure fastest possible recovery, there should be detailed instructions for each step in the recovery strategy.

The recovery strategy for “Identity Verification Provider permanently unavailable” cannot include “allow registrations without identity verification” as identity verification is a legal requirement for all customers. Instead, one feasible recovery strategy could include

- disabling new customer registrations.
- showing an informative message regarding disabled registrations.
- migrating to the pre-selected secondary identity verification provider.
- enabling new customer registrations.

More information on recovery strategies can be found in references [42][53]

Incident Response Plan

An Incident Response Plan (IRP) is a critical component that focuses specifically on minimising harm, protecting the company’s assets, and guaranteeing the success of immediate response and mitigation to previously identified risks or unforeseen incidents.

The Incident Response Plan requirements differ based on the industry, country, stage of the company and many other factors. For a cloud-native SaaS startup, the key areas to cover in the incident response plan are

- **Emergency Response Team:** Identifies the core personnel required in the case of emergency.
- **Incident Assessment:** Defines an systematic approach to assess the root cause, severity and impact of the incident.
- **Recovery Strategies**
- **Communication Plan:** Defines the communication plan and channels for regular status updates to key stakeholders (internal stakeholders, partners, customers, regulatory bodies)
- **Post-Incident Review (Postmortem):** A postmortem is an industry best practice approach to analysing and documenting significant incidents.

More information on Incident Response Planning can be found in references [50][51][52]

Emergency Response Team

Emergency response team includes the core personnel required in the case of emergency. When the key people have been selected and their responsibilities are documented, they can prepare and practice accordingly. For example, if two senior engineers are assigned the responsibility of database restoration using backups, they can practise the backup restoration regularly and make sure the relevant parts of the disaster recovery plan is up to date. [48][49]

The most important role of the emergency response team is **Incident Commander (IC)**[44], who leads the emergency response efforts and has the formal authority to make related decisions. The incident commander role is assigned based on the type of the incident. For example, the company's Chief Technology Officer (CTO) takes the role of the incident commander for any incident related to the company's SaaS service. Alternatively, the role can be assigned to the VP Of Engineering in case the CTO is not available. For any office space related incidents (e.g. employees cannot access the office, internet is down, office lost electricity), the incident commander role could be assigned to Chief Operating Officer (COO).

Incident Assessment

In the case of a sudden incident, it is important to quickly identify the root cause, severity, and impact of the incident, and plan the response and countermeasures accordingly. Major incidents are stressful events even for the most experienced employees. When the company's SaaS service is unavailable, there is a lot of pressure from all stakeholders and a sense of urgency to fix the issue as soon as possible. The emergency response team should be able to make rational and justified decisions even in the most stressful situations.

For example, data loss can be caused by multiple reasons like database crash, accidental deletion of data, bugs in the code, ransomware, or hackers gaining access to the system. While the outcome remains the same (data loss) the response to the incident differs greatly. If the team falsely identifies the source of data loss as accidental deletion of data by an employee, the data is highly likely to be lost again after the restoration if the real root cause was a bug in the code.

The incident assessment is a process of collecting relevant information of the incident that supports identifying the root cause. Each incident can be different and the process should be flexible and based on guidelines and best practices instead of strictly following a process that provides highly detailed instructions.

More information on incident assessment can be found in reference [47].

Post-Incident Review (Postmortem)

A postmortem is an industry best practice to analyse and document significant incidents, the related findings, and key learnings. It should also include action items to prevent similar incidents in the future. Postmortems are commonly shared to key stakeholders for reviews for transparency and to gain trust. [45]

4.3.4 Disaster Recovery Plan

A disaster recovery plan is a documented set of procedures designed to restore critical IT systems, data, and operations in the aftermath of a disruptive event (natural disaster, cyberattack, etc.), minimising downtime and ensuring business continuity. The disaster recovery plan provides detailed instructions for every step that is required to recover after a major incident and it should be tested regularly.

When creating a disaster recovery plan, the company must first define what is the maximum allowed time for the service to be unavailable in any given situation and how many hours of data loss the company is willing to tolerate in the case of an incident. These are defined using the following terms

- **Recovery Time Objective (RTO):** The maximum amount of downtime allowed in the case of an incident. Example: 12 hours
- **Recovery Point Objective (RPO):** The maximum tolerable amount of data loss measured in time. Example: 4 hours

With the example RTO and RPO times defined above, the service must be fully recovered, fully working, and accessible by customers within 12 hours from the start of the incident and data cannot be lost from a period of time that exceeds 4 hours.

After the RTO and RPO have been defined, the disaster recovery plan must be aligned to meet the objectives. The RPO target must also be reflected in the Data Retention Policy. If the RPO is 4 hours, the database backup interval must be 4 hours at maximum instead of the previously defined interval of 24 hours - otherwise the RPO cannot be met.

It might be tempting to define both RTO and RPO as low as possible, for example to 1 hour. This would require employee(s) to actively monitor the system 24 hours per day for 365 days per year and have an highly optimised

recovery process - and in most cases, the related costs greatly exceed the costs of 12 hour downtime and lost revenue.

Disaster recovery plan is a highly detailed technical documentation that provides step-by-step instructions for recovering from every possible major incident - may it be loss of the whole system, loss of a single component or database, or a ransomware attack. The previously mentioned documents (architecture documentation, service catalogue, risk assessment, data retention policy) helps greatly when creating disaster recovery plan as those documents provide details of the system, its components and data flows, external dependencies, and how and where data is stored, and the related risks.

The disaster recovery plan should be updated to include the new Identity Verification app, the new CloudSQL database and the integration to the Identity Verification Provider.

More information about the Disaster Recovery Plan can be found in references [24][25].

4.3.5 Incident Management Process

The risk assessment, business impact analysis, business continuity plan, and disaster recovery plan allows the startup to understand the risks, their impacts, how to continue operations, and how to recover from the incidents. An Incident Management Process is a process that encapsulates the actions required during the incident and to mitigate and resolve the incident [46].

A lightweight Incident Management process could be as follows [47]

- Detect the incident.
- Alert the Emergency Response Team.
- Assign the predefined roles.
- Set up communication channels (e.g. incident specific chat room for internal communications, email for customers and partners).

- Collect information from relevant systems and parties.
- Assess the impact and severity.
- Decide recovery strategy.
- Execute recovery actions.
- Document all taken recovery actions.
- Create a postmortem.

4.4 Managing Security

Security management is a subset of risk management and it follows the same process where the potential security threats are identified, analysed, assessed, prioritised and mitigated. In security management, the policies play a major role as those define the requirements and expectations. After the policies have been defined, those will guide the technical work to meet the defined requirements. For example, when a password policy is defined for the administrative UI user passwords, the engineering team should enforce the requirements by implementing or updating the related features.

The previously defined process is very suitable for technical security. The engineering team should identify, analyse, assess, prioritise and mitigate the security threats, document the findings and monitor the progress of implementation.

Table 8. A simplified Technical Risk Assessment.

RISK	CAUSE	IMPACT	MITIGATION	FREQUENCY	SEVERITY	DETECTABILITY	SCORE (RPN)
SQL Injection	Database queries use user input without proper sanitization.	Unauthorised access to data, data corruption, data deletion.	Use prepared statements, use stored procedures, sanitise user input.	2	5	3	30
Broken Authorization	Invalid authorization configuration,	Unauthorised access to data, data corruption,	Test authorization with unit, integration, and e2e tests.	2	5	5	50

	missing authorization configuration, missing authorization.	data deletion.	Add logging and monitoring.				

4.5 Managing Privacy and Personally Identifiable Information

Managing privacy and Personally identifiable information (PII) follows the same principles as risk and security management, but the requirements come often from the laws and regulations instead of the company's internal policies. Therefore it is important to understand and document the privacy requirements which may differ greatly between the markets. After the risks have been identified and assessed, and the mitigation strategies have been decided, the company should adjust its operations and modify its technical systems to meet the requirements.

4.5.1 EU General Data Protection Regulation (GDPR)

The EU General Data Protection Regulation (GDPR) is a comprehensive data privacy regulation that sets a global standard for the protection of personal data belonging to individuals within the European Union (EU) and European Economic Area (EEA). It aims to give individuals greater control over their personal information, including how it's collected, used, shared, and stored, while holding organisations accountable for responsible data handling practices and imposing significant penalties for non-compliance.

Under GDPR, a company can be either

- **Controller**: The controller is the entity that decides the purposes for which personal data is collected and processed, and how it is processed. The controller has the primary responsibility of the GDPR compliance, including the possible data processors.

- **Processor**: processes personal data on behalf of and under the instructions of the controller.

The example SaaS startup used in this thesis is a data controller. The startup has also the obligation to make sure any data processor (third-party entity) and service used for data processing meets the GDPR requirements.

To meet the EU GDPR requirements, the company should follow the following principles

- **Lawfulness, Fairness, and Transparency in data processing**: The data processing must have a valid legal basis, the data processing must be fair, and the organisations must be transparent about how the personal data is processed.
- **Purpose Limitation**: collecting data only for specified purposes
- **Data Minimization**: collecting only necessary data
- **Storage Limitation**: storing data only as long as it is needed
- **Security and confidentiality**: Protecting personal data from unlawful or unauthorised processing, accidental loss, destruction, or damage. Keeping personal data secret from unauthorised parties.
- **Accountability**: demonstrating compliance through documentation and procedures

Many of the requirements can be filled with previously introduced policies

- **Storage Limitation** is covered by **Data Retention Policy.**
- **Security and Confidentiality** is covered by **Data Retention Policy, User Data Access Policy, Password Policy, Secrets management Policy,** and **Encryption Policy.**
- **Accountability** and **Lawfulness, Fairness, and Transparency** can be partially achieved by the documentation and procedures introduced as part of this master's thesis.

More information about GDPR can be found in references [26][27].

4.5.1.1 GDPR Records Of Processing Activities

The GDPR Records of Processing Activities is a great document to cover the **Purpose Limitation**, **Data Minimization,** and parts of the **Lawfulness, Fairness, and Transparency** principles - assuming the startup considers the data it collects and the legal basis for doing so as part of the process.

The GDPR Records of Processing Activities is a mandatory document required under the General Data Protection Regulation that requires organisations to maintain comprehensive records of how they collect, process, store, and protect personal data of EU residents. This document includes information like the purpose of data processing, categories of data collected, who the data is shared with (third-parties), security measures in place, data retention periods, and details of the controller and processor of the data. The Records of Processing Activities demonstrate accountability and compliance with the GDPR's core principles of transparency and data protection.

The GDPR defines personal data as any information relating to an identified or identifiable natural person. An identifiable person is someone who can be identified by reference to an identifier [39]

- Direct identifiers are identifiers that can be used directly to identify a person: name, id number, location data, online identifiers (IP address, cookies), and others.
- Indirect identifiers are identifiers that can be used with other information to identify a person e.g. physical characteristics, job title and employer, financial information, genetic or biometric data, social or economic data.

If the company fails to be GDPR compliant, it can lead to significant financial sanctions or other penalties. For the most severe violations, the maximum fine is 20M€ or 4% of the company’s annual worldwide turnover. In less severe cases, the company can receive a warning or reprimand, a temporary or permanent user data processing ban and/or data erasure orders. [40][41]

Table 8. A simplified GDPR Records of Processing Activities.

PURPOSE OF PROCESSING	CATEGORIES OF DATA SUBJECTS	CATEGORIES OF PERSONAL DATA	DATA SHARING	LEGAL BASIS
To manage recruitment process	Job applicants	First name, last name, phone, email, resume/cv, background check results, work eligibility documents	TeamTailor Applicant Tracking System	Recruitment
Public website	Website visitors	IP Address, device/browser information,	Google Analytics	Consent
Public website	Contact form submissions	First name, last name, email, phone number	-	Contractual Necessity
To process customer payments and complete online orders.	Customers making online purchases	Name, credit card number, expiration date, CVV, billing address	Stripe	Contractual necessity (customer must pay to complete their subscription order)
Send promotional emails, newsletters, and personalised offers to subscribers	Customers who have opted in to receive marketing communications	Email address, name (optional), purchase history, website behaviour (with consent)	Mailchimp	Consent (freely given, specific, informed, and unambiguous)
To verify customer identities (legal requirement)	All customers	Name, birthday, identity card image, identity card unique identifier	Idenfy	KYC

As shown above, The GDPR Records of Processing Activities can meet the **Purpose Limitation**, **Data Minimization**, and **Lawfulness, Fairness, and Transparency** principles if the company decides to limit the amount of data collection and processing and do so only for a valid legal reason.

More information on the GDPR Records of Processing Activities can be found in reference [28].

An example GDPR Records of Processing Activities can be found in reference [29].

4.5.1.2 GDPR Rights

GDPR also grants the EU citizens many rights including, but not limited to [30]

- **Right to be Informed**: Organisations must provide clear and understandable privacy statements providing information what personal data is collected and why, how long it will be stored, and to whom the data is shared.
- **Right of Access**: The users have the right to have access to the collected data.
- **Right to Rectification**: The users can request their personal information to be corrected.
- **Right to be Forgotten**: The users have the right to request their personal data to be deleted (depending on the circumstances).
- **Right to Restrict Processing**: The users have the right to temporarily halt or limit how the company can use the user's data.
- **Right to Withdraw Consent**: The users have the right to withdraw previously granted consent for data collection and data processing. In an extreme case, this means the data collection and processing cannot be continued for any user who has withdrawn the consent.

The architecture documentation/diagram, data retention policy, and the GDPR Records of Processing Activities documents contribute greatly towards fulfilling these rights as the documents provide clear understanding what data is being collected and for how long, how it's processed, and how it's been shared to third parties. For example, when a user uses the **Right of Access** and requests a copy of the stored personal data, the documentation provides the necessary details to return a copy of the requested data. Additionally, if the system is well designed, it can automatically stop collecting, processing, and sharing the personal data when a user decides to use the **Right to Withdraw Consent**.

More information about GDPR rights can be found in reference [30].

4.5.1.3 GDPR Privacy Policy

GDPR Privacy Policy is a mandatory public facing document that is typically available on the company website. The Privacy Policy informs users how their personal data is collected, used, shared, and protected by the organisation. The Privacy Policy should be comprehensive and easy to understand. The Privacy Policy contributes towards the **Transparency** requirement of the GDPR.

The Privacy Policy should include at least the following [31]

- **Contact Information**: Company name and contact information.
- **Data Collected**: What data is being collected.
- **Purpose of Processing**: Why the data is being collected.
- **Legal Basis**: What is the legal basis for collecting and processing the data.
- **Recipients**: List of third-parties the company shares the data with.
- **Data Subject Rights**: Explain how users can exercise their GDPR rights (access, erasure, consent, etc).
- **Retention Periods**: How long is the data being stored.
- **Security Measures**: How the data is being secured.
- **Policy Changes**: How changes to the Privacy Policy will be communicated.

While the Privacy Policy is a comprehensive document, the previously defined policies and documentation simplify the drafting as those contain all the necessary details required in the GDPR Privacy Policy.

More information about GDPR Privacy Policy can be found in reference [31].

4.5.1.4 Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) under the GDPR is a process that helps organisations proactively identify and minimise the risks to individuals' personal data from new projects, technologies, or significant changes in how data is processed. DPIA is required when processing operations are “likely to result in a high risk to the rights and freedoms of natural persons” and it is an important tool for mitigating risks, and for demonstrating compliance with the GDPR. Typically, DPIAs are drafted as part of major projects that impact how the company processes data. A typical DPIA process is as follows [32]

- **Identify whether a DPIA is required**
- **Define the Data Processing**: Identify and Define the new data processing requirements, what kind of information will be used, and who can access it.
- **Identify Risks**: Perform a risk assessment; Identify, analyse, and assess potential risks that the project may expose to individuals and their rights or to the startup itself.
- **Define Mitigation Strategies**: Define mitigation strategies that will be used to mitigate the risks.
- **Sign-Off and Review**: Obtain sign-off from relevant stakeholders (CTO, DPO, legal).
- **Technical Implementation**: The DPIA should guide the technical implementation that should address the identified risks and defined mitigation strategies.

The DPIA is very similar to the previously introduced Risk Assessment and Business Impact Analysis. More information about Data Protection Impact Assessment can be found in reference [32].

4.6 Managing Work

Important part of the risk and security management process is managing the related work. Work management is the process of organising, assigning,

prioritising, tracking, and reporting on individual tasks required to complete a larger project or achieve ongoing goals. It's important because it provides structure and visibility into work, breaking down complex projects into manageable steps, ensuring tasks are completed on time and by the appropriate people, facilitating prioritisation, and promoting accountability, leading to overall improved efficiency and better outcomes.

For example, when a startup is building a new SaaS service and the launch date is close, the leadership of the company should be able to verify that all required work has been delivered and the company and the product are ready for the oncoming launch.

Most common project management tools can be used for managing the work. Additionally, some project management best practices should be followed

- **Organising**: Prioritising tasks, setting deadlines, and assigning them to team members.
- **Planning**: Breaking down projects into smaller, manageable tasks. Creating milestones with deliverables and delivery dates.
- **Tracking**: Monitoring work progress and identifying potential roadblocks.
- **Reviewing**: Most (if not all) risk and security related deliverables should be reviewed by other team members to verify its accuracy. For example, the emergency response team should review the disaster recovery plan when it’s been created or updated.
- **Reporting**: Communicating task status, progress, and results to stakeholders.
- **Ownership**: Each task should have a clear owner who is responsible for delivery.
- **Deadlines**: Each task should have a date when the work should be delivered at latest.
- **Status**: Each task should have a status.

The following example is based on Trello while many other common tools such as Microsoft Excel can be used too.

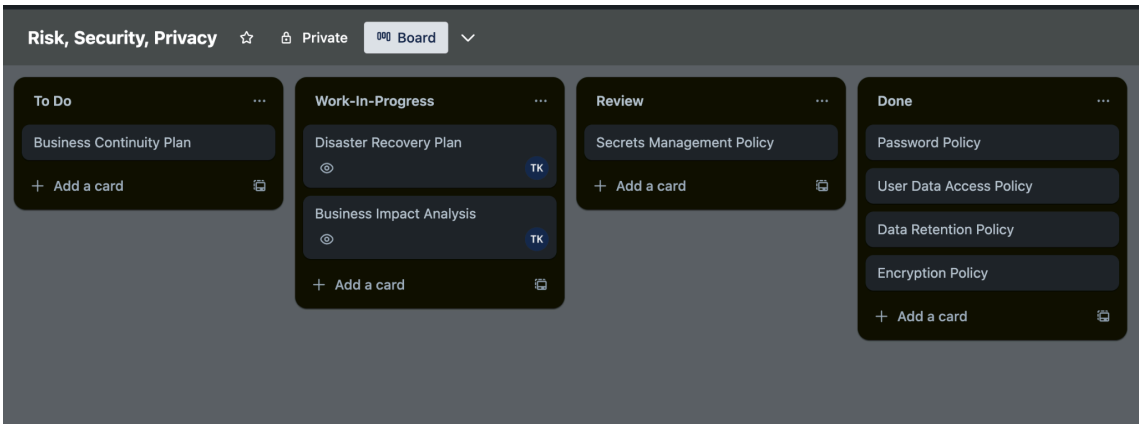

Figure 3. Project Management Tool.

When new work is identified, it should be immediately added to the tool. For example, the Identity Verification feature requires changes to multiple documents and individual tasks should be added to the project management tool to keep track of the work. For example, the following tasks could be added

- Update architecture documentation.
- Update service catalogue.
- Update GDPR Records of Processing Activities.
- Perform risk assessment.
- Perform business impact analysis.
- Perform business continuity plan.
- Perform DPIA if required.

After the tasks have been added to the selected tool, the work can be easily tracked to ensure it will be done.

5 Discussions and Conclusions

Risk and security management can be an overwhelming topic for anyone without formal training or prior experience. Even if a company would have an understanding of what risk and security management is and why it is important, it can be hard to know where to focus and how to get started.

The goal of this thesis was to address these issues and provide a baseline understanding of what risk and security management is, why it matters, what are the relevant documentation and processes, and how to include these in the daily operations.

As demonstrated in this thesis, it is possible to manage risk and security with limited knowledge. The startups can start with a limited scope, learn and gain experience, and then expand it to cover new areas while the company and business is growing. An additional finding was that the risk and security management can also contribute greatly towards the privacy management and provide a pathway to privacy and GDPR compliance.

The startup should document the initial state of their systems (architecture documentation, service catalogue) and draft the required policies (Password Policy, Data Retention Policy, User Data Access Policy, Secrets Management Policy, Encryption Policy). The next step is to identify the risks (Risk Assessment) and their impact (Risk Assessment, Business Impact Analysis), and how to recover and continue operations during an incident (Business Continuity Plan, Disaster Recovery Plan). Additionally, a common risk for any startup that has users or customers that are residents of the European Union, the GDPR compliance can be managed in a systematic manner.

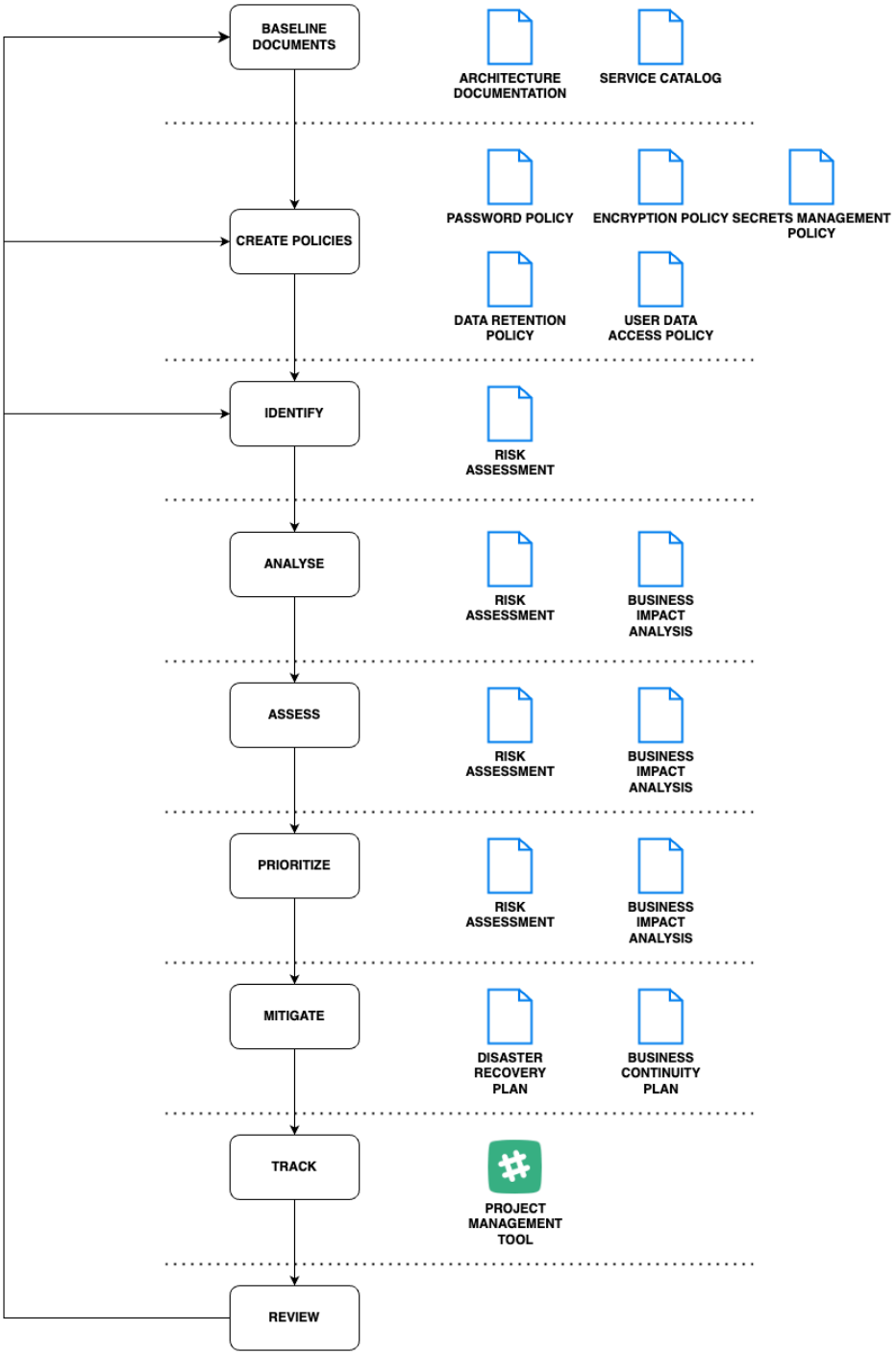

Figure 4. Risk and Security Management Process Diagram.

While this thesis investigated the problem from the perspective of a startup and its SaaS offering, it is possible to expand the framework to cover other key areas such as physical properties, employees, Intellectual Property (IP), or funding while the company and business grows.

The framework could be easily modified to support any other business too as the approach would still be somewhat similar: document the current status, identify and assess risks and the related business impact, design and implement mitigation strategies, and create continuity plans.

References

1 National Institute of Standards and Technology (NIST): Managing Information Security Risk <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf> Accessed 15 Jan 2024.

2 National Institute of Standards and Technology (NIST): Risk Management Framework for Information Systems and Organizations <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf> Accessed 15 Jan 2024.

3 National Institute of Standards and Technology: The NIST Cybersecurity Framework (CSF) 2.0 <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>. Accessed 10 Mar 2024.

4 National Institute of Standards and Technology: NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf>. Accessed 10 Mar 2024.

5 Center For Internet Security: CIS Critical Security Controls <https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf>. Accessed Feb 18 2024.

6 Information Security: The Ultimate Guide <https://www.imperva.com/learn/data-security/information-security-infosec/> Accessed Mar 9 2024

7 Scytale: Security Management Policy (IS Policy) <https://scytale.ai/glossary/security-management-policy-is-policy/> Accessed Mar 19 2024

8 Radix: Software Architecture Documentation: A Comprehensive Handbook <https://radixweb.com/blog/software-architecture-documentation-guide>. Accessed Feb 18 2024.

9 ServiceNow: What is an IT service catalog? <https://www.servicenow.com/products/itsm/what-is-it-service-catalog.html>. Accessed Feb 19 2024

10 Securden: Password Policy Recommendations for Sysadmins in 2023 <https://www.securden.com/blog/top-10-password-policies.html>. Accessed 10 March 2024.

11 Intradyn: Data Retention Policy 101: Best Practices, Examples & More <https://www.intradyn.com/data-retention-policy/>. Accessed March 20 2024.

12 SailPoint: Data access: What is it and why is it important? <https://www.sailpoint.com/identity-library/data-access/>. Accessed Feb 10 2024

13 Satori: What is the Purpose of a Data Access Control Policy? <https://satoricyber.com/data-access-control/what-is-the-purpose-of-a-data-access-control-policy/>. Accessed Feb 10 2024

14 Delinea: Secrets management: what is it and why is it important? <https://delinea.com/blog/secrets-management>. Accessed March 9 2024

15 OWASP: Secrets Management Cheat Sheet <https://cheatsheetseries.owasp.org/cheatsheets/Secrets_Management_Cheat_Sheet.html>. Accessed March 23 2024.

16 Amazon Web Services: General encryption best practices <https://docs.aws.amazon.com/prescriptive-guidance/latest/encryption-best-practices/general-encryption-best-practices.html>. Accessed Feb 8 2024.

17 Amazon Web Services: Creating an enterprise encryption strategy for data at rest <https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-data-at-rest-encryption/welcome.html>. Accessed Feb 8 2024.

18 Hyperproof: How to Perform a Successful IT Risk Assessment <https://hyperproof.io/resource/it-risk-assessment/>. Accessed Feb 2 2024.

19 Zerto: Risk Management Process- Part 2: Business Impact Analysis <https://www.zerto.com/blog/business-it-resilience/risk-management-process-part-2-business-impact-analysis/>. Accessed Feb 9 2024.

20 Asana: What is a business impact analysis (BIA)? 4 steps to prepare for anything <https://asana.com/resources/business-impact-analysis>. Accessed Feb 9 2024.

21 Zerto: Business Continuity - The Only Guide You Will Need <https://www.zerto.com/resources/essential-guides/business-continuity-guide/>. Accessed Feb 11 2024.

22 University Of Washington: GUIDE TO BUSINESS CONTINUITY AND RECOVERY PLANNING <https://www.ehs.washington.edu/system/files/resources/UWLabContinuityPlan.pdf>. Accessed April 7 2024.

23 Investopedia: What Is a Business Continuity Plan (BCP), and How Does It Work? <https://www.investopedia.com/terms/b/business-continuity-planning.asp>. Accessed March 2 2024.

24 Druva: Disaster recovery plan definition <https://www.druva.com/glossary/what-is-a-disaster-recovery-plan-definition-and-related-faqs>. Accessed March 3 2024.

25 Google: What is a Disaster Recovery Plan? <https://cloud.google.com/learn/what-is-disaster-recovery>. Accessed March 3 2024.

26 Data Protection Commission: GDPR for organisations <https://www.dataprotection.ie/en/organisations>. Accessed March 10 2024.

27 Data Protection Commission: Know Your Obligations <https://www.dataprotection.ie/en/organisations/know-your-obligations>. Accessed March 10 2024.

28 Data Protection Commission: Records of Processing Activities (RoPA) under Article 30 GDPR <https://www.dataprotection.ie/en/organisations/know-your-obligations>. Accessed March 10 2024.

29 Data Protection Commission: GDPR Records of Processing Activities template <https://assets.hse.ie/media/documents/gdpr-records-of-processing-activities-template.xlsm>. Accessed March 10 2024

30 Data Protection Commission: Your Rights under the GDPR <https://www.dataprotection.ie/en/individuals/rights-individuals-under-general-data-protection-regulation>. Accessed March 10 2024.

31 GDPR.EU: Writing a GDPR-compliant privacy notice <https://gdpr.eu/privacy-notice/>. Accessed March 10 2024.

32 Data Protection Commission: Data Protection Impact Assessments <https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments>. Accessed March 10 2024.

33 Varonis: What is a Security Policy? Definition, Elements, and Examples <https://www.varonis.com/blog/what-is-a-security-policy>. Accessed April 21, 2024

34 Kirkpatrickprice: 15 Information Security Policies Every Business Should Have <https://kirkpatrickprice.com/blog/15-must-have-information-security-policies/>. Accessed April 2, 2024

35 Webfargo: IT Security Policy Development <https://www.webfargo.com/it-security-policy-development.html>. Accessed April 2, 2024.

36 Alexander Setiawan, Adi Wibowo, Andrew Hartanto Susilo: Risk Analysis on the development of a Business Continuity Plan <https://www.researchgate.net/profile/Alexander-Setiawan-2/publication/323949453_Risk_analysis_on_the_development_of_a_business_continuity_plan/links/5b39b22b0f7e9b0df5e46a82/Risk-analysis-on-the-development-of-a-business-continuity-plan.pdf>. Accessed Feb 23, 2024.

37 Continuity2: What Are The Relationships Between Disaster Recovery, Risk Management and Business Continuity? <https://continuity2.com/blog/what-are-the-relationships-between-risk-management-business-continuity-and-disaster-recovery>. Accessed April 2 2024.

38 Relyence: How to assess risk using FMEA. <https://relyence.com/wp-content/uploads/2020/09/FMEA-Risk-Assessment-White-Paper.pdf>. Accessed Jan 23 2024.

39 GDPR.eu: What is considered personal data under the EU GDPR? <https://gdpr.eu/eu-gdpr-personal-data>. Accessed April 2 2024.

40 GDPR.eu: What are the GDPR Fines? <https://gdpr.eu/fines/>. Accessed April 2 2024.

41 European Commission: What if my company/organisation fails to comply with the data protection rules? <https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-companyorganisation-fails-comply-data-protection-rules_en>. Accessed April 2 2024.

42 BizCover: What is a business continuity plan? <https://www.bizcover.com.au/business-continuity-plan-guide/>. Accessed April 3 2024.

43 Agility: 10 Steps for Incident Management and Business Continuity <https://www.agilityrecovery.com/article/10-steps-incident-management-and-business-continuity>. Accessed March 10 2024.

44 Atlassian: Bringing order to chaos: The role of the incident commander <https://www.atlassian.com/incident-management/incident-response/incident-commander>. Accessed April 21 2024

45 Atlassian: How to run a blameless postmortem <https://www.atlassian.com/incident-management/postmortem/blameless> . Accessed April 21 2024.

46 Atlassian: What is incident management? <https://www.atlassian.com/incident-management#devops-and-sre-style-incident-management-process>. Accessed April 21 2024.

47 Atlassian: Incident Management Handbook <https://pages.eml.atlassian.com/rs/594-ATC-127/images/Atlassian-incident-management-handbook-.pdf>. Accessed April 21 2024.

48 IT Revolution: Building an Incident Management Response Team <https://itrevolution.com/articles/building-an-incident-management-response-team/>. Accessed April 21 2024.

49 Cynet: Incident Response Team: A Blueprint for Success <https://www.cynet.com/incident-response/incident-response-team-a-blueprint-for-success/>. Accessed April 21 2024.

50 Cynet: NIST Incident Response Plan: Process, Templates, and Examples <https://www.cynet.com/incident-response/nist-incident-response/>. Accessed Feb 22 2024.

51 NIST: Computer Security Incident Handling Guide <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>. Accessed Feb 22 2024.

52 TechTarget: Incident Response Plan <https://cdn.ttgtmedia.com/searchDisasterRecovery/downloads/SearchDisasterRecovery_Incident_Response_Plan_Template.doc>. Accessed Feb 22 2024.

53 Dino Cajic: Business Continuity Strategy <https://www.linkedin.com/pulse/business-continuity-strategy-dino-cajic-ejxxe/>. Accessed April 2 2024.