KPMG P/S
Dampfærgevej 28
2100 København Ø
Denmark

Telephone +45 70 70 77 60
www.kpmg.dk
CVR no. 25 57 81 98

Erhvervsstyrelsen

Security Analysis
Nordic Smart Government

July 2016
Security Analysis

Contents

1 Executive summary

1.1 Purpose

The purpose of this report is to deliver a high-level security analysis for an initial subset of the project Smart Government (SG).

The project SG aims to utilise the potential benefits of digitisation through automated exchange of data between authorities and businesses within each country in the Nordic region. SG will provide a way for authorities and relevant stakeholders to "pull" relevant data from companies, who already deposited the relevant underlying data in a cloud-based software solution. Effectively this will eliminate the need for businesses to prepare and file information multiple times.

The initial scope is limited to Small and Medium Enterprises (SME) providing data to a subset of governmental entities, but business to business communication and businesses providing data-services are taken into account as well. Companies in the SME segment are relatively more burdened by reporting than larger businesses, and likely do not have the means to maintain a full Business Intelligence (BI) system.

1.2 Results of the risk analysis

Based on a high-level security model, a risk analysis has been performed, and a range of mitigative controls have been analysed. The result of this analysis have been integrated into an overall security design for the SG system.

The high-level security model sets forth the following requirements:

- Data is ingested on a continuous basis
- Ingested data must be retrievable at any point in time or for any period (to use as basis for decisions or to prove correctness of decisions based on the data available at the time)
- Data should be tagged/classified on ingest (e.g. "Billing transaction")
- Rules for data retention, according to classification, should be created when changing the data plan (including how long raw data is needed and when aggregated data replaces raw data as sufficient legal grounds)
- Access should be granted to authenticated named entities/users (no shared access/anonymous)
- Authentication mechanism should support/integrate with existing governmental authentication frameworks
- Data access authorisation should be granted by the data owner (explicitly or implicitly)
- Data access authorisation should be (support being) granted for a time limited period (with start and end dates)
- Granted data access should be revocable

- Data access should be traceable, showing who has accessed a given data asset at a given time
- Data should be stored and transmitted in a manner that prevents circumvention of the authorisation mechanism.

The recommendations set forth are to implement Governance, Risk and Controls (GRC), managed through an Information Security Management System (ISMS) such as ISO 27001. This will form the basis for ensuring that the proposed mitigating controls are implemented and effective, as well as continuously adjusted to changes in the threat landscape.

1.3 Security design

Based on the risk assessment of the visionary design and the data model, the main focus of the security design is on preventing unauthorised access to and alteration of data. This is done through the following mitigating techniques:

- A policy defining responsibilities and ownership of data
- A framework for authorisation that is built on top of a mechanism for authentication
- A principle of granting minimal access based on need
- Technical protection based on encryption of data at rest and during transport
- Technical protection based on principles for secure code development
- Technical protection based on segregation of test/development and production systems combined with data obfuscation (stripping, anonymisation and pseudonymisation)
- Reactive controls to identify if the access controls are being circumvented, such as Logging, Intrusion Detection and Prevention Systems, machine learning to locate irregular access patterns, etc.

Further focus is put on availability of data, which is done through the following mitigating techniques:

- Implementation of Change and Capacity Management processes
- Implementation of backup and restore procedures
- Implementation of general operational procedures and event management process.

It should be noted that the availability aspect would potentially become more critical with a broader system scope where e.g. business critical transactions (ordering parts, invoicing, etc.) are supported, as downtime could disrupt the supply chain of the individual businesses.

1.4 Conclusion

If these recommendations are adhered to, further developed and implemented effectively, we deem that it is possible to create an SG environment in which data is handled in a manner that prevents unauthorised access and data loss while still providing the envisioned benefits to enterprises and government institutions.

This is, however, dependent on the future selected IT architecture, which should be risk assessed as part of the development process.

1.5 Suggested next step

Our recommended next step is to create a general requirement specification for the SG system, in which the functional as well as non-functional (e.g. security) requirements are fleshed out. This specification could be shared among the Nordics, allowing relevant areas to be adjusted for specific national requirements.

Once the requirement specification has developed, next steps could likely be to implement a Proof-of-Concept system in which the selected product and actual implementation can be tested and evaluated. The Nordic countries could choose either do this as a joint project, or as national projects according to needs and preferences.

Due to the modular and dynamic way data is stored, we expect it to be possible to expand the PoC system once it has reached a sufficient maturity level, rather than reimplement for a bigger scope.

2 Background, Scope and Methodology

2.1 Background

In April 2016, Erhvervsstyrelsen (ERST) requested KPMG to perform a high-level security analysis for the project Smart Government (SG). Concurrently, ERST requested Deloitte to perform a high-level data-model analysis.

The project Smart Government (SG) aims to utilise the potential benefits of digitisation through automated exchange of data between authorities and businesses within each country in the Nordic region. SG may provide a way for authorities and relevant stakeholders to "pull" relevant data from companies, who already deposited the relevant underlying data in a cloud-based software solution. Effectively this will eliminate the need for businesses to prepare and file information multiple times.

The business drivers described in the vision papers are:

- To create a single point of financial reporting for a company, off-loading much of the administrative work from the company and automating it.
- To enable continuous reporting of data in order to
    - get increased insight into current status of businesses
    - create up-to-date statistical data on which to base (e.g. fiscal political) decisions
    - perform automated fraud detection/risk response through machine learning.
- To implement an open framework in order to
    - let any relevant vendor integrate into the framework
    - enable an extensible data model that allows stakeholder-specific changes to the data plan, i.e. allow the possibility of extending the types of data that entities can upload and share based on future needs.
    - increase the service offerings relating to and business value of uploaded data
    - support increased digitisation and value to companies.

2.2 Scope

The scope defined for this initial security analysis is as follows:

- Stakeholders are limited to Small and Medium Enterprises (SME) providing data to a subset of governmental entities consisting of the Tax Authorities, Business Authorities and Statistical Authorities.
  These companies are relatively more inconvenienced by reporting and likely do not have the means to maintain their own BI systems.
- Data is limited to financial data, billing data, accounting data, data from digital communication with businesses and data from preliminaries (such as tax files from businesses).

To ensure future expansion the model also considers the possible data exchange between businesses (B2B) as well as the possibility of businesses to act as data-service vendors (BI).

2.3 Methodology

The methodology applied to perform the Security Analysis is based on the following steps:

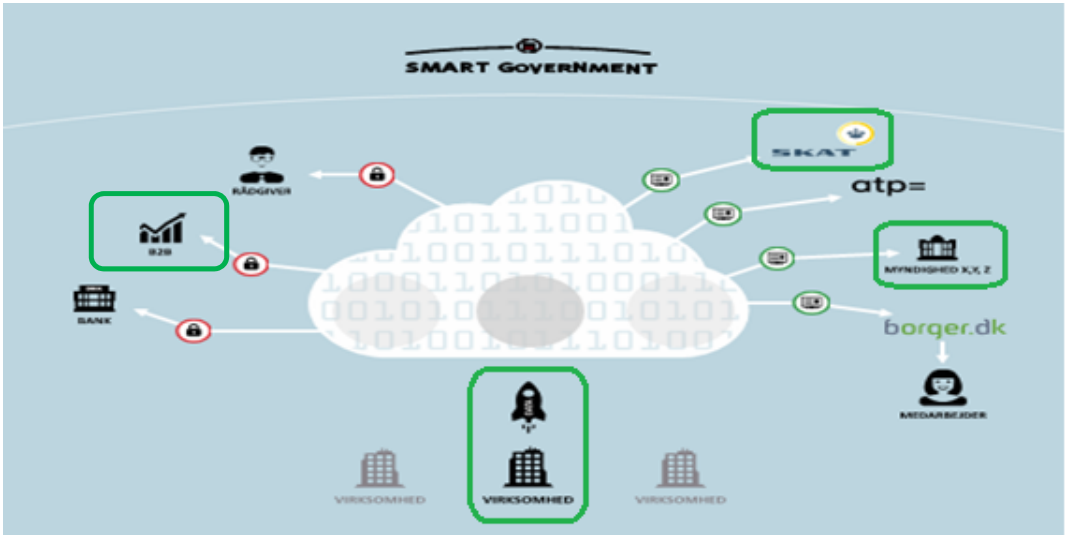
- Design security principles
  Based on project documentation and interviews with the ERST team, high-level security principles and associated stakeholders are identified.
- Create risk model
  Relevant threats, threat actors, vulnerabilities, events, etc. are scoped.
  Based on the identified principles and the performed scoping, a relevant risk framework is selected.
- Perform risk assessment
  The risk model is applied to the scoped threats, etc., and possible mitigation techniques are evaluated.
- Design security model
  One or more security models are suggested based on the assessed risks and the proposed mitigation techniques.
- Put model in Nordic perspective
  The model is put under high-level assessment in relation to differing legislation across the Nordics.
- Provide recommendations
  A set of security recommendations including implementation recommendations and best practice are set forth.

3 High-level Security Model

In order to assess risks to the data assets, the Smart Government vision has been modelled into abstract components that interact with data assets.

3.1 The Smart Government vision

The main "cloud" vision as described in the paper "Visionspapir om Smart Government – 120115" is shown below with the primary stakeholders (SME's, Tax Authorities, Business Administration Authorities and Statistical Authorities) indicated.



Although the primary focus has been on the entities that would be involved in a "basis implementation" (simplifying the SME's reporting to government entities), the extended usage scenarios have not been ignored. The security model has been generalised to an extent where the risk assessments of data access by government entities also covers enterprise (B2B & BI) access.

Based on the business drivers listed in section 2 and best practices, a set of high-level security principles can be defined.

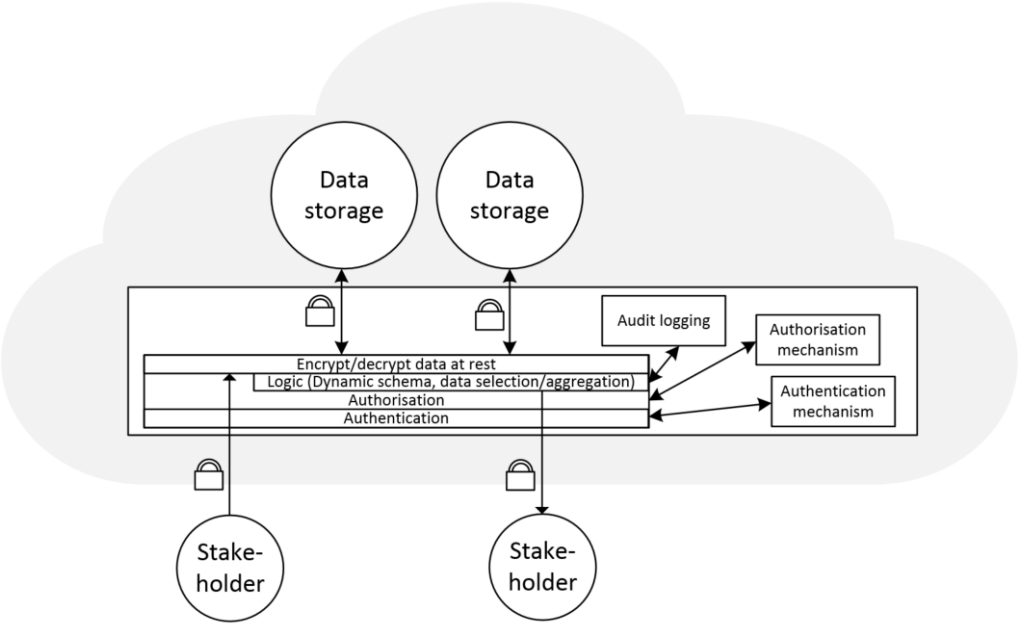
3.1.1 High-level security principles

The model should adhere to the following high-level security principles:

- Data is ingested on a continuous basis.
- Ingested data must be retrievable at any point in time or for any period (to use as basis for decisions or to prove correctness of decisions based on the data available at the time).
- Data should be tagged/classified on ingest (e.g. "billing transaction").

- Rules for data retention according to classification should be created when changing the data plan (Including how long raw data is needed and when aggregated data replaces raw data as sufficient legal grounds).
- Access should be granted to authenticated named entities/users (no shared/anonymous access).
- Authentication mechanism should support/integrate with existing governmental authentication frameworks.
- Data access authorisation should be granted by the data owner (explicitly or implicitly).
- Data access authorisation should be (support being) granted for a time limited period (with start and end dates).
- Granted data access should be revocable.
- Data access should be traceable, showing who has accessed a given data asset at a given time.
- Data should be stored and transmitted in a manner that prevents circumvention of the authorisation mechanism.

The in-scope parts have been modelled in the following way:



The data store contains the data at rest, while stakeholders upload or download data through a middleware layer. The model allows for future scope expansion where businesses can download data as well, since both the businesses and the authorities have been modelled in the same way.

The business uploading data retains ownership of the raw data. Once data is aggregated and downloaded, ownership of the resulting data transfers to the aggregating party.

The security model can only handle data inside the SG system – once authorisation to download raw data has been given, and data has left the SG security environment, security has to be maintained on the downloading system by the downloading stakeholder.

4 Risk Framework and Assessment

To assess the risk level of the envisioned system and design mitigating controls, a relevant risk framework needs to be selected.
Due to the high-level nature of the current design, the risk framework should not be based on a quantitative approach. Rather, a qualitative approach should be used, in which an opinion- and scenario-based rating system is used to assess risk criticality levels.

A selection of international frameworks has been considered (NIST 800-30, FRAP, OCTAVE, FMEA, CORAS). The risk framework that has been selected is OCTAVE Allegro, based on several factors:

- It has a wide approach, contemplating the entire system and not just parts thereof.
- It is not focussed on technology, which is an advantage when no actual technology has been decided.
- It is focussed on information assets.
- It does not require extensive involvement from the data or system owners (at this level of abstraction)
- It includes risk mitigation considerations as part of the model.

OCTAVE Allegro can be used in conjunction with ISO/IEC 27005, the ISO/IEC 27000 standard for information security management systems (ISMS), as the ISO/IEC 27005 does not specify a specific risk model to be used.

4.1 Risk analysis approach

The OCTAVE Allegro framework consists of an eight-step methodology, based on four distinct areas:

- Establish drivers, where the organisation develops risk measurement criteria that are consistent with organisational drivers.
- Profile assets, where the assets that are the focus of the risk assessment are identified and profiled and the assets' containers are identified.
- Identify threats, where threats to the assets – in the context of their containers – are identified and documented through a structured process.
- Identify and mitigate risks, where risks are identified and analysed based on threat information, and mitigation strategies are developed to address those risks.

4.1.1 Establish drivers

Step 1. Establish Risk Measurement Criteria

In order to assess the individual risks, the criteria for measuring impact has to be defined.

This is covered in three main areas:

- Reputation and customer confidence, covering the impact relating to trustworthiness and political support.
- Financial, covering operating cost and the ability to invoice taxes, etc.
- Fines and legal penalties, covering risk of conflicts with legislation.

The identified areas are then prioritised based on expected impact to the SG system. The prioritisation is used later in the model to assign an overall risk value to individual threat scenarios.

Additional information of the specific implementation of this step is available in Appendix B.1.

4.1.2 Profile assets

Step 2. Develop an Information Asset Profile

As the vision is very high-level, the information assets have been defined by the scope:

Aggregated and transactional level information from businesses to the authorities for Tax, Business Administration and Statistics, as well as B2B and BI usage.
The data is not defined closely, but will contain Personal Identifiable Information (PII) and financial data.

Additional information of the specific implementation of this step is available in Appendix B.2.

Step 3. Identify Information Asset Containers

Once the information assets have been identified, the information flow is analysed to assess where the data is stored or handled (i.e. the information asset containers). In the context of the model of the SG vision, this leads to the following asset containers (grouped by data state):

Data at rest:

- Data storage, internal (SG repository of raw data and reports)
- Data storage, external (external stakeholder having downloaded data)
- Backup media, internal and external (where copies of data is stored for recovery purposes)

Data in transit:

- Internal network (network connecting SG components)
- External network (where the data is transmitted from SG to stakeholders, e.g. the Internet)

Data in use:

- IT staff, internal (with privileged access to SG internals)

- IT staff, external (with privileged access to downloaded data, and to software that interacts with SG)
- BI staff (with access to perform analysis on data)

Additional information of the specific implementation of this step is available in Appendix B.3.

4.1.3 Identify threats

Step 4. Identify Areas of Concern

Based on the identified data assets and asset containers, the following areas of concern have been identified:

- A data owner disappears (e.g. stakeholder bankrupts/closes down).
- A stakeholder is unable to access data (that he should have access to).
- A stakeholder uploads false data.
- Data integrity is compromised.
- Data confidentiality is compromised.
- Data is used in a manner not in accordance with granted permission of use.
- Data is not retained/deleted according to retention scheme.
- Employee privileges too broad/high.
- Data is unavailable or lost due to system failure.
- Data storage overloaded.
- System compromised.

Each of these areas is to be analysed as individual threat scenarios.

Step 5. Identify Threat Scenarios

For each area of concern possible threat scenarios consisting of an actor, means and motive are described.

Example scenarios are:

- An employee disables access to the system servers by shutting down servers for personal gain.
- An employee discloses information that he has access to by accident.
- A stakeholder performs data aggregation at a level that exposes confidential data.
- An employee deletes data by accident.
- System failure causes partial or full shutdown.

4.1.4 Identify and mitigate risks

Step 6. Identify Risks

For each of the threat scenarios, the outcome is determined based on four categories: Disclosure, Modification, Destruction and Interruption. Furthermore, it is determined what security requirement was breached.

Examples are:

- (An employee deletes data by accident) causes destruction of data and potentially interruption of service, which could breach the security requirements for "data access granted based on need" and availability.
- (System failure) potentially causes interruption or destruction of data, which could breach the security requirement for availability.

Additional information of the specific implementation of this step and all risks, one per each table is available in Appendix B.8.

Step 7. Analyse Risks

The Risks are further analysed based on estimated consequences and severity, resulting in a Relative Risk Score (a priority).

For each threat scenario, an impact score for the individual impact areas (as defined in step 1) is calculated by multiplying the impact area rank with the scenarios assessed impact value on the given area.

The total Relative Risk Score is the sum of the individual impact scores for the scenario.

The overall relative risk scores are as follows:

System compromised	18
Unauthorised access to data	15
A stakeholder is unable to access data (that he should have access to)	13
System failure causes unavailability and/or data loss	13
Data's integrity compromised	12
Data deleted	9
System storage overloaded	9
A company went bankrupt leading to the situation where there is no one left to grant access to the company's data	6
A stakeholder uploads false data	6
Unintended data usage	6

Showing that the primary threat is external actors trying to breach the system, closely followed by internal actors accessing data without authorisation. As external actors often abuse internal actors' access privileges, controls focusing on access privileges would mitigate both.

Step 8. Select Mitigation Approach

Based on the Relative Risk Scores and the assessed probability of each scenario occurring, a risk matrix is constructed and available in Appendix B.6. This is used for prioritising the areas where mitigation is needed.

Based on the analysed risks a risk response action is selected. The possible actions are:

- Accept
  A decision made during risk analysis to take no action to address a risk and to accept the stated consequences. Risks that are accepted should have little to low impact on the organisation.

- Defer
  A situation where a risk is neither accepted nor mitigated based on the organisation's desire to gather additional information and perform additional analysis. Deferred risks are monitored and re-evaluated at some point in the future. Risks that are deferred are generally not an imminent threat to the organisation nor would they significantly impact the organisation if realised.

- Mitigate
  A decision made during risk analysis to address a risk by developing and implementing controls to counter the underlying threat or to minimise the resulting impact, or both. Risks that are mitigated are those that typically have a medium to high impact on an organisation.

- Transfer
  A financial risk may be mitigated by transferring it, i.e. take out an insurance policy against the treat.

In this analysis, all but one scenario have resulted in a number of mitigative actions. Only the risk(s) caused by a data owner going out of business has been deferred. This scenario requires further analysis to ensure that the consequences are handled adequately in relation to legislation, transfer of ownership, responsibilities, etc. before a set of supporting controls can be designed.

The mitigative actions are shown grouped as part of the high-level security design.

An overview of all mitigation techniques outlined throughout the risk analysis with regards to each identified risk is available in Appendix B.7.

5 High-level Security Design

Based on the risk analysis, the primary risk to take into consideration is breach of confidentiality - unauthorised access to information, either by an external or internal agent. Further main risks are related to availability, which in this scope scores relatively low, but could score much higher in a future scenario where SG is expanded to transport e.g. invoicing or other transactions directly related to businesses daily operation and liquidity. The third major risk is to data integrity – that data is not tampered with once it has been entered into SG.

If an initial implementation is based on voluntary participation by the individual companies (and thus explicit approval of data usage), legislation seemingly presents little or no problem regarding data collection.

Once the participation in SG becomes mandatory, or it is decided to require access to raw data without the owner granting explicit permission, the right to data access must be anchored in the legislation. An analysis of the required data access must be based on the relevant authorities' actual need for aggregated data, which will likely change over time as more possibilities for insight are explored.

It should be noted that the Security Design only covers the SG system. Once data leaves the system, it is no longer covered by the internal security controls, but has to rely on the information security design at the external entity. Information security requirements at external stakeholders could be supported/enforced by contracts or legislative requirements.

In order to manage the entire set of controls, including the continuous review and updating of policies, procedures and technical controls, an Information Security Management System (ISMS) should be implemented. A common European standard is ISO 27001, which is either mandatory or recommended for governmental institutions across the Nordics.

The first step in the ISMS is to define the roles and responsibilities relating to the system. This includes, but is not limited to:

- How is the governance structure constructed
- Segregation of Duties requirements
- Who is data owner, and when and how is ownership transferred
- Who is responsible for user access management
- Who is responsible for information security management and internal audit?

In order to manage data access, it is necessary to implement a set of controls including organisational (procedures for granting, revoking and reviewing access) and technical (authentication of users, authorisation of access rights to read, alter or delete data).

To detect possible circumvention of the access controls, technical controls (event logging, audit logging, Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS)) should be implemented and procedures put in place for regularly review and response (preferably as part of a Security Information and Event Management (SIEM) System).

The granularity of access control has to be defined as well, which includes segregation in system components and networks. Test and development environments should be segregated

from the production environment, and data obfuscation/anonymisation employed on data used outside the production environment.

In order to increase availability and prevent unapproved changes to the system, a formalised process for Change Management should be enforced. Furthermore, Capacity Management should be implemented in order to proactively handle capacity requirements.
These preventive measures should be complemented by operational supervision of the systems by an Event Management process to detect operational failures or potential failures.

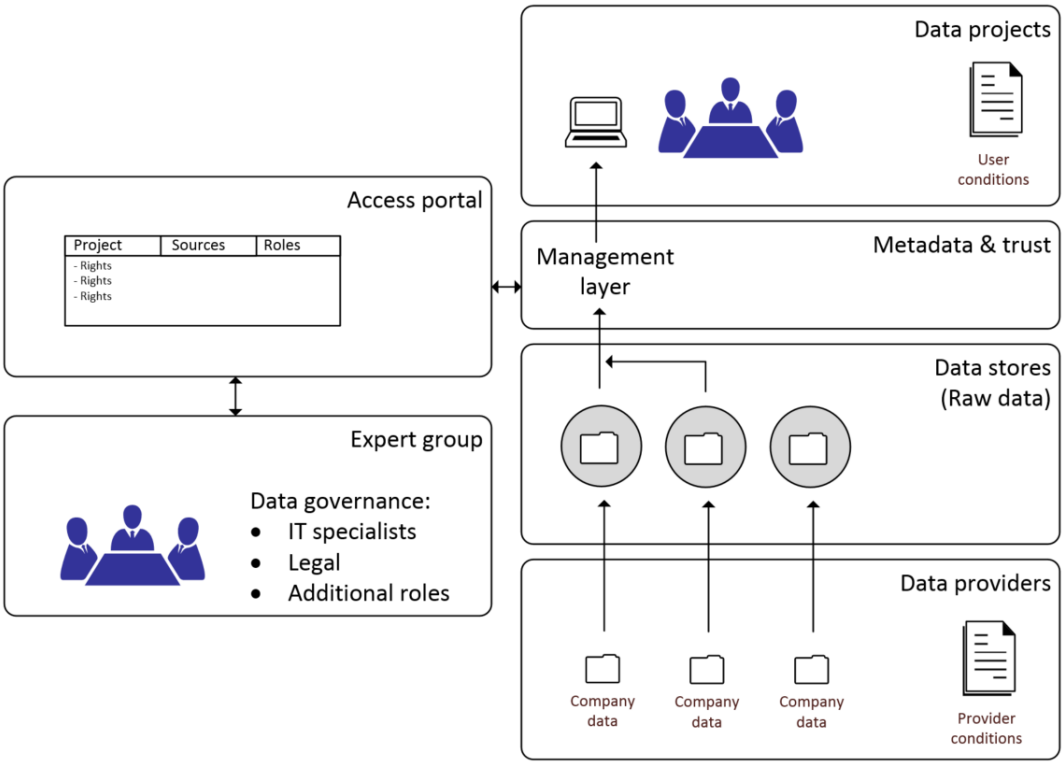
As a general best practice approach, we recommend that well-known international risk control standards such as CIS 20 Critical Security Controls (formerly SANS 20), NIST 800-53, DSD top 35 and CSA cloud control matrix are used as guidance for the implementation of operational controls.

Presenting the logical organisation of the system from a different angle, the system is split into multiple raw data stores, each with a data owner (the uploading part).
On top of these is an overarching "virtual data store", where the "logic" is placed. The logic is able to perform searches and aggregations across the individual data stores. This logic is what the receiving part uses for extracting data from the system.

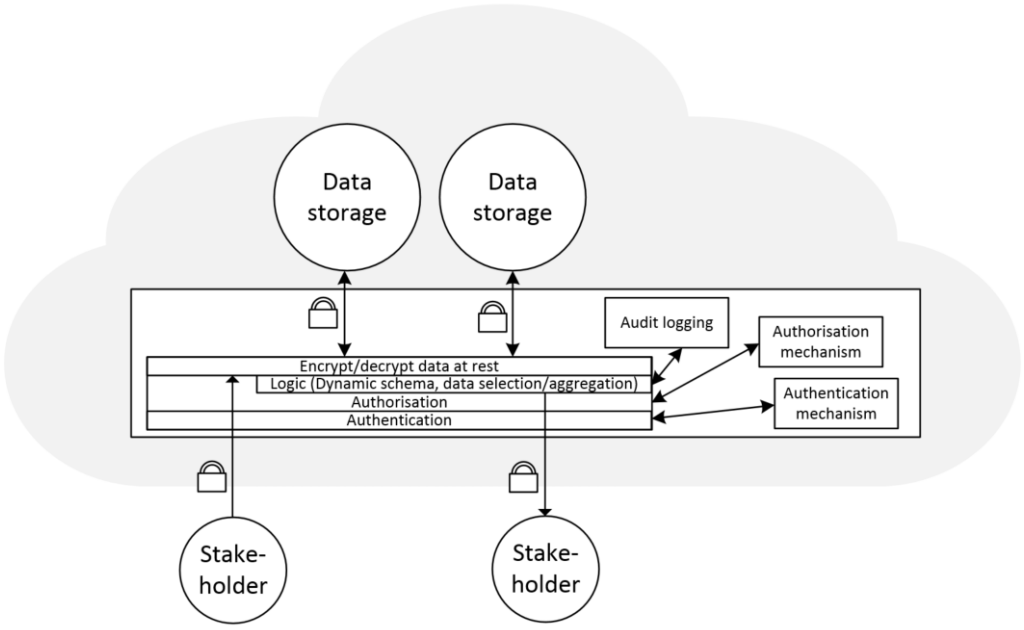
Access is managed in three layers:

- At the owner
  the uploading *data owner* maintains control of who has access to the data in the individual data store.
- At the user
  the downloading *data user* is assigned a certain role.
- At the logic level
  Permission must be granted for a role to use a specific piece of logic on a specific data store.

The logic is created and maintained by a group of internal specialist staff, whose access should be controlled as discussed earlier. The access rules should be controlled by an expert group.



Revisiting the system model, we will take a closer look at the components and relate them to the mitigation techniques selected in the risk assessment.



The purposes and functionality of the three mechanisms shown (Authentication, Authorisation and Logging) are described in detail below, as are the encryption layers.

5.1 Authentication

The purpose of the authentication system is to ensure that the user/entity requesting access is who he claims to be. Knowledge of the exact identity of the user is a requirement for ensuring that access is granted only to relevant users, as well as for maintaining an audit trail of who has had access to data at any given time.

The authentication mechanism should integrate with any existing authentication framework standard used by the government. This could be e.g. (OIO)SAML, as used in Denmark, Norway, and Sweden.

As the data store authentication mechanism may be different from the existing authentication framework, the SG system should have the ability to bridge the systems and map between identities.

5.2 Authorisation

The purpose of the authorisation system is to ensure that the user is only allowed access to information based on the authorisations that he has been granted.

The authorisation framework must support the data model – a collection of mixed data indexed via a data dictionary. This means that the authorisation framework must be able to handle access to data based on data attributes.

Furthermore, the authorisation model has to support data access based on user attributes (i.e. the user belongs to a certain organisation, has a specific role, connects from a trusted location, etc.)

Finally, the authorisation framework has to support granting access based on "a specific purpose/usage of data", i.e. is based on a policy.

We recommend applying an Attribute Based Access Control (ABAC) authorisation scheme to support this. An ABAC grants access based on attributes of the user, the data and an access policy, and thus extends the older and more common Role Based Access Control (RBAC). Some ABAC implementations (e.g. XACML) are designed to integrate with SAML authentication, which would make it fit into the (OIO)SAML scheme currently in use.

5.3 Logging

The purpose of logging is twofold:

- Logging as a means to discover errors or abuse as it happens (event logging).
- Logging data access as a means to document who has accessed what data (audit logging).

The event logging covers system events as well as user actions and should be logged and monitored in a Security Information and Event Management (SIEM) system. This will enable

quicker identification, analysis and recovery of security events. As a supplement to static event-patterns, machine-learning algorithms could be applied to identify irregular data access.

This would implement the mitigating controls relating to Intrusion Detection and Intrusion Prevention Systems (IDS/IPS).

The audit logging will be more extensive, as it will have to log access to any data. The primary purpose is to have a trusted trail of events, and the objective is to save the data in a secure, non-alterable way. The integrity of the logs could be handled through a number of techniques, including distributed ledger techniques (blockchains). Audit logging can be integrated with the ABAC rule system to ensure approved and denied access are logged.

5.4 Encryption

Encryption protects sensitive and valuable data at rest and in motion by transforming plaintext into coded form – cipher text. When employed it works as an almost invisible part of employed communication protocols. Essentially, it provides another layer of protection against data theft or breaches on cloud infrastructure (such as inadvertent data leakage during storage or transfer or through deliberate data harvesting by the cloud provider). The following are the principles regarding encryption that are required to meet the security goals:

- Encrypt data at rest
- Transmit data only with secure protocols.

For data encryption at rest, we recommend following best practice, e.g. using symmetric-key cryptography such as Advanced Encryption Standard (AES), with a complexity (key length) that reflects the data criticality.

For transmission, we also recommend following best practice, e.g. usage of public-key cryptography such as Transport Layer Security (TLS).

5.5 Recovery

In order to recover from data loss created by system failure, user error or malicious actions, a backup and recovery scheme should be set up. This requires defining allowable data loss and data recovery times, as well as implementing procedures for backup.

Note should be taken that backups also contain data-at-rest and should be protected by e.g. encryption.

6 Conclusions & recommendations

Based on the security analysis, a high-level security design has been presented. If the recommendations presented in the design are adhered to, further developed and implemented effectively, we deem that it is possible to create an SG environment in which data is handled in a manner that prevents unauthorised access and data loss while still providing the envisioned benefits to enterprises and government institutions.

This is, however, dependent on the future selected IT architecture, which should be risk assessed as part of the development process.

The implementation must be based on a sound technological design, supported by a GRC implementation that ensures that technical as well as organisational controls are in place.

A range of controls has been recommended and should be taken into account when designing the IT architecture.

Our recommended next step is to create a general requirement specification for the SG system, in which the functional as well as non-functional (e.g. security) requirements are fleshed out. This specification could be shared among the Nordics, with some areas adjusted for specific national requirements.

Once the requirement specification has been fleshed out, next steps could likely be to implement a Proof-of-Concept system in which the selected product and actual implementation can be tested and evaluated. The Nordic countries could either do this as a joint project, or as national projects according to needs and preferences.

Due to the modular and dynamic way data is stored, we expect it to be possible to expand a PoC system once it has reached a sufficient maturity level, rather than reimplement for a bigger scope.

A Abbreviations

Advanced Encryption Standard	AES
Attribute Based Access Control	ABAC
Business Intelligence	BI
Business to Business	B2B
Governance, Risk and Controls	GRC
Erhvervsstyrelsen	ERST
Information Security Management System	ISMS
Intrusion Detection System	IDS
Intrusion Prevention System	IPS
Proof of Concept	PoC
Security Assertion Markup Language	SAML
Security Information and Event Management System	SIEM
Small and Medium Enterprises	SME
Smart Government	SG
Transport Layer Security	TLS

B Appendix

B.1 Qualitative Measures

Risk Measurement Criteria - Reputation and Customer Confidence			
Impact Area	**Low**	**Moderate**	**High**
Reputation (with regards to stakeholders and political origins)	Reputation is minimally affected; little or no effort or expense are required to recover	Reputation is damaged, and some effort and expense are required to recover	Reputation is irrevocably destroyed or damaged
Political impact	Minimal impact; little or no effort or expense are required to recover	Political storm	Political figure forced to resign from post

Risk Measurement Criteria - Financial			
Impact Area	**Low**	**Moderate**	**High**
Operating costs	Increase of less than 0-1% in yearly operating costs	Increase of less than 1-5% in yearly operating costs	Yearly operating costs increase by more than 5%
Revenue loss	Less than 1% yearly revenue loss	1-5% yearly revenue loss	Greater than 5% yearly revenue loss
One-time financial loss	One-time financial cost of less than 10,000 €	One time financial cost of 10,000 to 50,000 €	One-time financial cost greater than 50,000 €

Risk Measurement Criteria - Fines and Legal Penalties			
Impact Area	**Low**	**Moderate**	**High**
Fines	Fines less than 5,000 €	Fines between 5,000 to 10,000 €	Fines greater than 10,000 €
Investigations	No queries from government or other investigative organisations	Government or other investigative organisation requests information or records	Government or other investigative organisation initiates a high-profile, in-depth investigation into organisational practices

	Priority
3	Reputation
2	Fines
1	Financial

B.2 Assets

Critical Information Asset Profile		
(1) **Critical Asset** What is the critical Information asset?	(2) **Rationale for Selection** Why is this information asset important to the organisation?	(3) **Description** What is the agreed-upon description of this information asset?
Small and Medium-sized Enterprise Data (SMED)	**This system is the main driver of the infrastructure. Challenges can result in customers experiencing issues with their normal functioning**	**The asset contains all the data that stakeholders submit such as financial and personal data, billing codes and payment history**
(4) **Owner(s)** Who owns this information asset?		
Each stakeholder owns its own data		
(5) **Security Requirements** What are the security requirements for this information asset?		
Confidentiality	Only authorised personnel can view this information asset	**Stakeholders have read access to their own records as well as those records where access has been explicitly granted by the owner through a request form**
Integrity	Only authorised personnel can modify this information asset	**It is critical to the entire infrastructure to provide integrity of the data stored in there. The only authorised personnel to perform any modification should be the data owner**
Availability	This asset must be available for 24 hours, 7 days/week, 52 weeks/year	**The asset should always be available as data submission and especially invoicing services will be running around the clock. Even short outages can cause significant problems depending on the time of the day**
Other (data must have an active owner)	This asset must have an active owner at any time.	**The data access is approved by the data owner. If access cannot be granted to new stakeholders, the data will be (unintentionally) unavailable to them**

Other (correctness)	Uploaded data is correct	**The data in the system is used by business authorities, therefore the correctness of the data must be ensured**
Other (regulatory compliance)	This asset has special regulatory compliance protection requirements	**The private data stored in the asset contains personal data of the company employees, such as social security numbers, which are subject to EU data protection regulations**

(6) **Most important Security Requirement** What is the most important security requirement for this information asset?

	Confidentiality	**Integrity**	**Availability**	**Other**	

B.3 Information Containers

Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	**Owner(s)**
1. Data Storage: Contains all data submitted by stakeholders.	SG owner
2. Internal Network: All the enterprise data travels through this network.	SG owner
External	
Container Description	**Owner(s)**
1. The Internet: The main medium through which all the data is transferred from the enterprise to the system and vice versa.	Unknown
2. Data Storage: The data storage is residing here after it has been downloaded by a stakeholder or before it has been uploaded to the system.	The stakeholder

Information Asset Risk Environment Map (Physical)	
Internal	
Container Description	**Owner(s)**
1. Backup tapes of the data storage are created and stored after a fixed interval.	SG owner
External	
Container Description	**Owner(s)**
1. Backup tapes of the downloaded data are created and stored after a fixed interval.	The stakeholder

Information Asset Risk Environment Map (People)	
Internal Personnel	
Name or Role/Responsibility	**Department or Unit**
1. IT Staff: The person working as system or data administrator has access to the system.	SG owner
External Personnel	
Contractor, Vendor, etc.	**Organisation**
1. Stakeholder's IT Staff: People working on behalf of stakeholders, be it the entity uploading the data or the entity downloading the data, have access to credentials as well as the data.	Stakeholders
2. Stakeholder's BI Staff: People working on behalf of stakeholders who perform data aggregation for BI or similar.	Stakeholders

B.4 Threats

Areas of concern:
A data owner disappears (What happens with the data, who owns it afterwards?)
A stakeholder is unable to access data (which he should have access to)
A stakeholder uploads false data
Data's integrity compromised
Unauthorised access to data/data's confidentiality compromised (during transportation or in the DB)
Unintended data usage
Data deleted/not deleted prior to the * years of which it should be kept
Over-privileged employees (Employee grants unapproved access to a stakeholder)
System failure causes unavailable and/or data loss
System storage overloaded
System compromised

B.5 Risk Overview

Risk #	Risk name	Risk score
10	System compromised	18
5	Unauthorised access to data	15
2	A stakeholder is unable to access data (which he should have access to)	13
8	System failure causes unavailability and/or data loss	13
4	Data's integrity compromised	12
7	Data deleted	9
9	System storage overloaded	9
1	Data has no owner (due to data owner disappearing)	6
3	A stakeholder uploads false data	6
6	Unintended data usage	6

B.6 Risk matrix

The risk number is placed in the squire accordingly to the probability and the risk score in the matrix.

Relative Risk Matrix			
Probability	Risk score		
	0 - 6	7 - 12	13 - 18
High	1		10
Medium	3	9	5 8
Low	6	4 7	2

B.7 Mitigations

An overview of mitigation techniques and the risk sheets in which they are relevant.

Mitigation/Risk number	1	2	3	4	5	6	7	8	9	10
Limit both physical and remote access to the data storage on need to have basis		x								
Limit both physical and remote access to the network equipment on need to have basis		x								
Data validation to ensure the correctness of the data to an acceptable degree			x							
Machine learning to locate patterns suggesting incorrect (by purpose or accidental) data			x							
Limit the access to the database storage on need to have basis				x	x		x			X
Encrypt data at rest, so that modification would result in broken data, which will require the stakeholder to re-upload (but since the data will appear broken if the encrypted value is modified, it will not result in any further misuse of it).				x						
Ensure data is transferred via encrypted means between middle layer and storage				x	x					
Ensure data is transferred via encrypted means between stakeholder and middle layer				x	x					
Encrypt the data in rest					x					X
Notify external stakeholders (through a warning when they access confidential data that they have previously obtained permission to) that they are about to access confidential data and it should be treated with caution, advise them on using encrypted mediums to store it and limit the access to it					x					
Ensure that all backups are encrypted					x					
Ensure that any staff involved understands the risks of accidentally or intentionally exposing confidential data					x					
Create policies regarding data transportation, whether it is "over the wire" or through external devices (such as usb flash sticks or hard drives), so that the data is always protected/encrypted					x					
Audit logging					x					
Awareness and legislative requirements					x	x				
Do not disclose BI data without an expert's verification that it cannot be misused or have other unintended usage						x				

Enforce BI rules that ensure aggregated data is based on population big enough to prevent deduction of individual stakeholder data						x				
Ensure backups are taken at an acceptable time range; thus in case of emergency data can be recovered without any loss							x			
Permit only data invalidation, not data deletion							x			
Apply multi-step approval before deletion of data							x			
Perform quality assurance and testing on a test environment before deploying new updates or features (rather than directly in production). Ensure that all functionality is tested after each modification before it is being deployed								x		
Implement change management procedures, including test requirements								x	x	
Ensure that the network bandwidth can handle the expected traffic to the system and deploy anti-denial of service attack tools. Deploy network-monitoring tools								x		
Implement capacity and event management procedures and deploy technical controls against DoS								x	x	
Implement backup procedures and assess the need relating to RPO/RTO								x		
Contractual agreement on automatic storage extension									x	
Deploy all CIS 20 Critical Security Controls where possible										X
Perform regular penetration testing and vulnerability scanning of the system as a whole										X
Ensure network segregation and raw access to the database only from the internal network										X
Ensure network monitoring and deploying Intrusion Detection and Protection Systems										X
Use public-key cryptography for critical access and 2-factor authentication for users										X
Ensure that every operation to the database escapes user input and does not result in a web vulnerability such as OWASP TOP 10										X
Ensure that decryption keys are stored on a separate medium, encrypted themselves										X

B.8 Risk worksheets

B.8.1 Risk 1

Information Asset Risk Worksheet					
Information Asset Risk	Threat	**Information Asset**	SMED		
		Area of Concern	A company went bankrupt leading to the situation where there is no one left to grant access to the company's data.		
		(1) Actor Who would exploit the area of concern or threat?	Third Party		
		(2) Means How would the actor do it? What would they do?	Due to financial reasons the company goes bankrupt.		
		(3) Motive What is the actor's reason for doing it?	Non-intentional, the company goes out of business		
		(4) Outcome What would be the resulting effect on the information asset?	☐ Disclosure	☐ Destruction	☑ Interruption / ☐ Modification
		(5) Security Requirements How would the information asset's security requirements be breached?	This asset must have an active owner at any time.		
		(6) Probability What is the likelihood that this threat scenario could occur?	☑ High	☐ Medium	☐ Low
	(7) Consequences What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?		**(8) Severity** How severe are these consequences to the organization or asset owner by impact area?		
			Impact Area	**Value**	**Score**
	If the company goes bankrupt then as there is no one from the company to grant access to company's historical data it will be difficult to get access to it.		**Reputation & Customer Confidence (3)**	Low(1)	3
			Financial (1)	Low(1)	1
			Fines & Legal Penalties (2)	Low(1)	2
			Relative Risk Score		6

(9) Risk Mitigation			
Based on the total score for this risk, what action will you take?			
☐ Accept	☑ Defer	☐ Mitigate	☐ Transfer
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	What administrative, technical and physical controls would you apply on this container? What residual risk would still be accepted by the organization?		

B.8.2 Risk 2

Information Asset Risk Worksheet						
Information Asset Risk	Threat	**Information Asset**	SMED			
		Area of Concern	A stakeholder is unable to access data(that he should have access to).			
		(1) Actor Who would exploit the area of concern or threat?	Staff			
		(2) Means How would the actor do it? What would they do?	Physically/remotely disable, shutdown, destroy or limit access to the system server(s) and/or network connection.			
		(3) Motive What is the actor's reason for doing it?	Personal			
		(4) Outcome What would be the resulting effect on the information asset?	☐ Disclosure	☐ Destruction	☐ Modification	☑ Interruption
		(5) Security Requirements How would the information asset's security requirements be breached?	This asset must be available for 24 hours, 7 days/week, 52 weeks/year			
		(6) Probability What is the likelihood that this threat scenario could occur?	☐ High	☐ Medium	☑ Low	
	(7) Consequences What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?		**(8) Severity** How severe are these consequences to the organization or asset owner by impact area?			
			Impact Area	**Value**	**Score**	
	The system will be unavailable for data extraction		**Reputation & Customer Confidence (3)**	High(3)	9	
			Financial (1)	Medium(2)	2	
			Fines & Legal Penalties (2)	Low(1)	2	
			Relative Risk Score		13	

(9) Risk Mitigation			
Based on the total score for this risk, what action will you take?			
☐ Accept	☐ Defer	☑ Mitigate	☐ Transfer

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	What administrative, technical and physical controls would you apply on this container? What residual risk would still be accepted by the organization?
Data Storage(Internal)	Limit both physical and remote access to the data storage on need to have basis.
Network (Internal)	Limit both physical and remote access to the network equipment on need to have basis.

B.8.3 Risk 3

Information Asset Risk Worksheet					
Information Asset Risk	Threat	**Information Asset**	**SMED**		
		Area of Concern	A stakeholder uploads false data		
		(1) Actor Who would exploit the area of concern or threat?	The stakeholder who uploads data.		
		(2) Means How would the actor do it? What would they do?	Follow the normal procedure however the data in the system is incorrect.		
		(3) Motive What is the actor's reason for doing it?	Personal Accidental		
		(4) Outcome What would be the resulting effect on the information asset?	☐ Disclosure ☑ Modification	☑ Destruction ☐ Interruption	
		(5) Security Requirements How would the information asset's security requirements be breached?	The data in the system must be correct.		
		(6) Probability What is the likelihood that this threat scenario could occur?	☐ High	☑ Medium	☐ Low
	(7) Consequences What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?		**(8) Severity** How severe are these consequences to the organization or asset owner by impact area?		
			Impact Area	**Value**	**Score**
	Any further analysis, such as BI or performed by financial authorities will result in incorrect scales.		**Reputation & Customer Confidence (3)**	Low(1)	3
			Financial (1)	Low(1)	1
			Fines & Legal Penalties (2)	Low(1)	2
			Relative Risk Score		6

(9) Risk Mitigation			
Based on the total score for this risk, what action will you take?			
☐ Accept	☐ Defer	☑ Mitigate	☐ Transfer

For the risks that you decide to mitigate, perform the following:	
On what container would you apply controls?	**What administrative, technical and physical controls would you apply on this container? What residual risk would still be accepted by the organization?**
Data Storage(Internal)	Data validation to ensure the correctness of the data to an acceptable degree.
Data Storage(Internal)	Machine learning to locate patterns suggesting incorrect (by purpose or accidental) data

B.8.4 **Risk 4**

Information Asset Risk Worksheet					
Information Asset Risk	Threat	**Information Asset**	SMED		
		Area of Concern	Data's integrity compromised		
		(1) Actor Who would exploit the area of concern or threat?	Staff		
		(2) Means How would the actor do it? What would they do?	Access and modify data		
		(3) Motive What is the actor's reason for doing it?	Personal		
		(4) Outcome What would be the resulting effect on the information asset?	☐ Disclosure ☐ Destruction ☑ Modification ☐ Interruption		
		(5) Security Requirements How would the information asset's security requirements be breached?	Only authorized personal can modify this data.		
		(6) Probability What is the likelihood that this threat scenario could occur?	☐ High	☐ Medium	☑ Low
	(7) Consequences What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?		**(8) Severity** How severe are these consequences to the organization or asset owner by impact area?		
			Impact Area	**Value**	**Score**
	Any further analysis, such as BI or performed by financial authorities will result in incorrect scales.		**Reputation & Customer Confidence (3)**	Medium(2)	6
			Financial (1)	Medium(2)	2
			Fines & Legal Penalties (2)	Medium(2)	4
			Relative Risk Score		12

(9) Risk Mitigation			
Based on the total score for this risk, what action will you take?			
☐ Accept	☐ Defer	☑ Mitigate	☐ Transfer
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	What administrative, technical and physical controls would you apply on this container? What residual risk would still be accepted by the organization?		
Data Storage (Internal)	Limit the access to the database storage on need-to-have basis.		
Data Storage (Internal)	Encrypt data at rest, so that modification would result in broken data which will require the stakeholder to re-upload(But since the data will appear broken if the encrypted value is modified, it will not result in any further misusage of it).		
Network (Internal)	Ensure data is transferred via encrypted means		
Network (External)	Ensure data is transferred via encrypted means		

B.8.5 **Risk 5**

Information Asset Risk Worksheet					
Information Asset Risk	Threat	**Information Asset**	SMED		
		Area of Concern	Unauthorized access to data		
		(1) Actor Who would exploit the area of concern or threat?	Staff or Third-party partner		
		(2) Means How would the actor do it? What would they do?	An employee might disclose confidential information that he has access to. Third-party partners(service providers, BI stakeholders etc) are known to be careless with confidential data, thus it is possible that they store it in a cloud solution, send it through an unencrypted medium or simply disclose it to unauthorized parties.		
		(3) Motive What is the actor's reason for doing it?	Accidental, Personal or Entertainment		
		(4) Outcome What would be the resulting effect on the information asset?	☑ Disclosure	☐ Destruction	
			☐ Modification	☐ Interruption	
		(5) Security Requirements How would the information asset's security requirements be breached?	Only authorized personnel can view this information asset		
		(6) Probability What is the likelihood that this threat scenario could occur?	☐ High	☑ Medium	☐ Low
	(7) Consequences What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?		**(8) Severity** How severe are these consequences to the organization or asset owner by impact area?		
			Impact Area	**Value**	**Score**
	Exposure to stakeholder's confidential data to the public will result in lawsuits and fines for breaches.		**Reputation & Customer Confidence (3)**	High(3)	9
	The public's overall perception of the system's quality could be negatively affected if private data gets exposed.		**Financial (1)**	Medium(2)	2
			Fines & Legal Penalties (2)	Medium(2)	4
			Relative Risk Score		15

(9) Risk Mitigation			
Based on the total score for this risk, what action will you take?			
☐ Accept	☐ Defer	☑ Mitigate	☐ Transfer
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	What administrative, technical and physical controls would you apply on this container? What residual risk would still be accepted by the organization?		
Data Storage (Internal)	Limit the access to the database on need-to-have basis.		
Data Storage (Internal)	Encrypt the data in rest.		
Data Storage (External)	Notify external stakeholders(through a warning when they access confidential data that they have previously obtained permission to) that they are about to access confidential data and it should be threated with concious, advice them on using encrypted mediums to store it and limit the access to it.		
Network (Internal and External)	Enable encryption for any transport medium, whether it is internal or external access to the database, which will reduce the risk of exposure to network captures		
Network (Internal and External)	Enable logging, and ensure policy that the logs are reviewed regularly. This will reduce the likelihood of an insider activity and increase the likelihood that an outsider activity will be detected.		
Back up tapes	Ensure that all backups are encrypted.		
Staff (Internal and External)	Ensure that any staff involved understands the risks of accidently or intentianally exposing confidential data.		
Staff (Internal and External)	Create policies regarding data transportation whether it is "over the wire" or through external devices (such as usb flash sticks or hard drives), so that the data is always protected/encrypted.		
Data Storage (Internal)	Audit logging		
Stakeholders BI-staff	Awareness and legislative requirements		

B.8.6 **Risk 6**

Information Asset Risk Worksheet					
Information Asset Risk	Threat	**Information Asset**	SMED		
		Area of Concern	Unintended data usage		
		(1) Actor Who would exploit the area of concern or threat?	Third-party stakeholder		
		(2) Means How would the actor do it? What would they do?	Perform data aggregation, which can result in exposing a stakeholder's confidential data.		
		(3) Motive What is the actor's reason for doing it?	Accidental Personal		
		(4) Outcome What would be the resulting effect on the information asset?	☑ Disclosure	☐ Destruction	☐ Modification ☐ Interruption
		(5) Security Requirements How would the information asset's security requirements be breached?	Only authorized personnel can view this information asset		
		(6) Probability What is the likelihood that this threat scenario could occur?	☐ High	☐ Medium	☑ Low
	(7) Consequences What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?		**(8) Severity** How severe are these consequences to the organization or asset owner by impact area?		
			Impact Area	**Value**	**Score**
	Exposure of stakeholder's confidential data to the public or to another stakeholder that can deduct the values by performing analytic calculations		**Reputation & Customer Confidence (3)**	Low(1)	3
			Financial (1)	Low(1)	1
			Fines & Legal Penalties (2)	Low(1)	2
			Relative Risk Score		6

(9) Risk Mitigation			
Based on the total score for this risk, what action will you take?			
☐ Accept	☐ Defer	☑ Mitigate	☐ Transfer
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	What administrative, technical and physical controls would you apply on this container? What residual risk would still be accepted by the organization?		
Stakeholder's BI Staff	Do not disclose BI-data without an expert's verification that it cannot be misused or have other unintended usage.		
Stakeholder's BI Staff	Legislation (not allowed to use data for other purposes than those granted access for)		
Enforce BI-rules that ensures aggregated data is based on population big enough to prevent deduction of individual strakeholder data			

B.8.7 **Risk 7**

Information Asset Risk Worksheet					
Information Asset Risk	Threat	**Information Asset**	SMED		
		Area of Concern	Data deleted		
		(1) Actor Who would exploit the area of concern or threat?	Staff		
		(2) Means How would the actor do it? What would they do?	Accessing stored data and deleting it.		
		(3) Motive What is the actor's reason for doing it?	Personal gain Accidental		
		(4) Outcome What would be the resulting effect on the information asset?	☐ Disclosure	☑ Destruction	
			☐ Modification	☑ Interruption	
		(5) Security Requirements How would the information asset's security requirements be breached?	Only authorized personnel can modify this information asset		
		(6) Probability What is the likelihood that this threat scenario could occur?	☐ High	☐ Medium	☑ Low
	(7) Consequences What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?		**(8) Severity** How severe are these consequences to the organization or asset owner by impact area?		
			Impact Area	**Value**	**Score**
	Data destroyed and it is unavailable to be used for its intended purpose.		**Reputation & Customer Confidence (3)**	Medium(2)	6
			Financial (1)	Medium(1)	1
			Fines & Legal Penalties (2)	Medium(1)	2
			Relative Risk Score		9

(9) Risk Mitigation			
Based on the total score for this risk, what action will you take?			
☐ Accept	☐ Defer	☑ Mitigate	☐ Transfer
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	What administrative, technical and physical controls would you apply on this container? What residual risk would still be accepted by the organization?		
Data Storage (Internal)	Limit the access to need-to-have basis and allow data deletion only if authorized by the owner of the data.		
Back up tapes	Ensure backups are taken at acceptable time range thus in case of emergency data can be recovered without any loss.		
Data Storage (Internal)	Permit only data invalidation, not data deletion.		
Data Storage (Internal)	Apply multi-step approval before deletion of data		

B.8.8 **Risk 8**

Information Asset Risk Worksheet					
Information Asset Risk	Threat	**Information Asset**	SMED		
		Area of Concern	System failure causes unavailability and/or data loss		
		(1) Actor Who would exploit the area of concern or threat?	System Failure		
		(2) Means How would the actor do it? What would they do?	Unexpected behaviour causes the system to shut down partly or fully.		
		(3) Motive What is the actor's reason for doing it?	Failure		
		(4) Outcome What would be the resulting effect on the information asset?	☐ Disclosure	☑ Destruction	
			☐ Modification	☑ Interruption	
		(5) Security Requirements How would the information asset's security requirements be breached?	This asset must be available for 24 hours, 7 days/week, 52 weeks/year		
		(6) Probability What is the likelihood that this threat scenario could occur?	☐ High	☑ Medium	☐ Low
	(7) Consequences What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?		**(8) Severity** How severe are these consequences to the organization or asset owner by impact area?		
			Impact Area	**Value**	**Score**
	The system will be unavailable for data extraction		**Reputation & Customer Confidence (3)**	High(3)	9
	If a crash occurs before the data is backed up, it will be lost		**Financial (1)**	Medium(2)	2
			Fines & Legal Penalties (2)	Low(1)	2
			Relative Risk Score		13

(9) Risk Mitigation			
Based on the total score for this risk, what action will you take?			
☐ Accept	☐ Defer	☑ Mitigate	☐ Transfer
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	What administrative, technical and physical controls would you apply on this container? What residual risk would still be accepted by the organization?		
Internal Storage	Perform quality assurance and testing on a test environment before deploying new updates or features (rather than directly in production). Ensure that all functionality is tested after each modification before it being deployed. Implement change management procedures, including test requirements		
Network (Internal)	Ensure that the network bandwidth can handle the extected traffic to the system and deploy Anti - Denial of Service attack tools. Deploy network monitoring tools.		
Network (Internal)	Implement capacity and event management procedures and deploy technical controls against DoS		
Internal Storage	Implement backup procedures and assess the need relating to RPO/RTO		

B.8.9 **Risk 9**

Information Asset Risk Worksheet					
Information Asset Risk	Threat	**Information Asset**	SMED		
		Area of Concern	System storage overloaded		
		(1) Actor Who would exploit the area of concern or threat?	System Failure		
		(2) Means How would the actor do it? What would they do?	The data storage is overloaded		
		(3) Motive What is the actor's reason for doing it?	Failure		
		(4) Outcome What would be the resulting effect on the information asset?	☐ Disclosure ☐ Destruction ☐ Modification ☑ Interruption		
		(5) Security Requirements How would the information asset's security requirements be breached?	This asset must be available for 24 hours, 7 days/week, 52 weeks/year		
		(6) Probability What is the likelihood that this threat scenario could occur?	☐ High	☑ Medium	☐ Low
	(7) Consequences What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?		**(8) Severity** How severe are these consequences to the organization or asset owner by impact area?		
			Impact Area	**Value**	**Score**
	The system becomes unavailable due to overloaded storage.		**Reputation & Customer Confidence (3)**	Medium(2)	6
			Financial (1)	Low(1)	1
			Fines & Legal Penalties (2)	Low(1)	2
			Relative Risk Score		9

(9) Risk Mitigation			
Based on the total score for this risk, what action will you take?			
☐ Accept	☐ Defer	☑ Mitigate	☐ Transfer
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	What administrative, technical and physical controls would you apply on this container? What residual risk would still be accepted by the organization?		
Data Storage (Internal)	Implement capacity and event management procedures		
Data Storage (Internal)	Implement change management procedures, and make sure capacity demands are adressed in changes		
Data Storage (Internal)	Contractual agreement on automatic storage extention		

B.8.10 **Risk 10**

Information Asset Risk Worksheet					
Information Asset Risk	Threat	**Information Asset**	SMED		
		Area of Concern	System compromised		
		(1) Actor Who would exploit the area of concern or threat?	Staff, Third-party partner or Unknown		
		(2) Means How would the actor do it? What would they do?	Gaining partial or full unauthorized access/control over the system		
		(3) Motive What is the actor's reason for doing it?	Political Personal Entertainment		
		(4) Outcome What would be the resulting effect on the information asset?	☑ Disclosure ☑ Modification	☑ Destruction ☑ Interruption	
		(5) Security Requirements How would the information asset's security requirements be breached?	Confidentiality, Integrity, Availability, Other		
		(6) Probability What is the likelihood that this threat scenario could occur?	☑ High	☐ Medium	☐ Low
	(7) Consequences What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?		**(8) Severity** How severe are these consequences to the organization or asset owner by impact area?		
			Impact Area	**Value**	**Score**
	Data can be disclosed, modified or deleted.		**Reputation & Customer Confidence (3)**	High(3)	9
	The system can be shut down or tampered with to become unavailable for unknown period of time.		**Financial (1)**	High(3)	3
	The public's overall perception of the system's quality could be negatively affected if it gets compromised.		**Fines & Legal Penalties (2)**	High(3)	6
			Relative Risk Score		18

(9) Risk Mitigation	
Based on the total score for this risk, what action will you take?	
☐ Accept ☐ Defer ☑ Mitigate ☐ Transfer	
For the risks that you decide to mitigate, perform the following:	
On what container would you apply controls?	What administrative, technical and physical controls would you apply on this container? What residual risk would still be accepted by the organization?
Data Storage (Internal)	Ensure that access to the database is given only if necessary and on need-to-have basis and authentication scheme using public-key cryptography for critical access and 2-factor authentication for users.
Data Storage (Internal)	Ensure that every operation to the database escapes user input and does not result in a web vulnerability such as OWASP TOP 10.
Data Storage (Internal)	Ensure data at rest is encrypted and the decyption keys are stored on a separate medium, encrypted themselves.
Network (Internal)	Ensure network segregation and raw access to the database only from the internal network.
Network (Internal)	Ensure network monitoring and deploying Intrusion Detection and Protection Systems.
Other	Perform regular penetration testing and vulnerability scanning of the system as a whole.
Deploy all CIS 20 Critical Security Controls where possible.	
Data Storage (Internal)	Encrypt data at rest
Data Storage (Internal)	Grant access to the data based on need-to-have basis