**IT Audit**

**Report**

****

Nick van Oort, Max Post

& Arwen Voorn

**3-6-2021**

# Document History

## Revisions

Table 0‑1 - Revisions

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Status | Date | Change |
| 0.1 | Concept | 30-4-2021 | The first draft of the document. |
| 0.2 | Concept | 11-5-2021 | Feedback Tom Jacobs (EY) processed. |
| 0.3 | Concept | 25-5-2021 | Feedback Atos processed. |
| 1.0 | Final | 1-6-2021 | The final version of the document. |

## Approval

This document requires the following approvals:

Table 0‑2 - Approval

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Approval date | Name | Function |
| 1.0 | 1-6-2021 | Atos | Client |

## Distribution

This document has been distributed to:

Table 0‑3 - Distribution

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Distribution date | Name | Function |
| 0.1 | 4-5-2021 | Tom Jacobs | Auditor (EY) |
| 0.2 | 18-5-2021 | Atos | Client |
| 0.3 | 1-6-2021 | Atos | Client |

Contents

[Document History 2](#_Toc73534705)

[Revisions 2](#_Toc73534706)

[Approval 2](#_Toc73534707)

[Distribution 2](#_Toc73534708)

[Management summary 5](#_Toc73534709)

[1 Introduction 6](#_Toc73534710)

[1.1 Project description 6](#_Toc73534711)

[1.2 Standard framework and scope 6](#_Toc73534712)

[1.3 Particularities project 7](#_Toc73534713)

[2 IT Audit 8](#_Toc73534714)

[2.1 Research Questions 8](#_Toc73534715)

[2.1.1 Main Question 8](#_Toc73534716)

[2.1.2 Sub Questions 8](#_Toc73534717)

[2.2 ISMS (Information Security Management System) 8](#_Toc73534718)

[3 Results 9](#_Toc73534719)

[3.1 Sub-question 1: What are the risks for the designed information architecture? 9](#_Toc73534720)

[3.1.1 Risk Analysis 9](#_Toc73534721)

[3.1.2 Quantified likelihood 9](#_Toc73534722)

[3.1.3 Acceptance criteria & Impact analysis 10](#_Toc73534723)

[3.1.4 Quantified risk assessment 12](#_Toc73534724)

[3.2 Sub-question 2: What is the impact of the risks if the framework isn’t applied? 13](#_Toc73534725)

[3.2.1 Relation between risks and quality aspects 13](#_Toc73534726)

[3.3 Sub-question 3: Advice on how to use the guidelines from the framework to assess data security? 16](#_Toc73534727)

[3.3.1 Control measures 16](#_Toc73534728)

[3.3.2 Quantitative risk assessment 19](#_Toc73534729)

[4 Conclusion 20](#_Toc73534730)

[4.1 Prioritization 20](#_Toc73534731)

[4.2 Advice 20](#_Toc73534732)

[Appendix 21](#_Toc73534733)

[Appendix A – Risk Analysis 21](#_Toc73534734)

[Appendix B – Control Measures 26](#_Toc73534735)

[Encrypting and Signing 26](#_Toc73534736)

[Bibliography 28](#_Toc73534737)

List of tables and figures

**Tables**

[Table 0‑1 - Revisions 2](#_Toc73534738)

[Table 0‑2 - Approval 2](#_Toc73534739)

[Table 0‑3 - Distribution 2](#_Toc73534740)

[Table 2‑1 - PDCA-cycle 8](#_Toc73534741)

[Table 3‑1 - Acceptance criteria 10](#_Toc73534742)

[Table 3‑2 - Quality Aspect 13](#_Toc73534743)

[Table 3‑3 - ISO 27001: A.10: Cryptography 16](#_Toc73534744)

[Table 3‑4 - ISO 27001: A.13.2: Information transport 17](#_Toc73534745)

[Table 3‑5 - ISO 27001: A.17.1: Information security continuity 18](#_Toc73534746)

[Table A-0‑1 - Meaning behind the likelihood risk scores 21](#_Toc73534747)

**Figures**

[Figure 1‑1 - Object 6](https://stichtingfontys.sharepoint.com/sites/ICTBusiness-Semester6697/Gedeelde%20documenten/PROF%20-%20Company%205/ATOS/ITA/ITA%20Rapport.docx#_Toc73534748)

[Figure 3‑1 - Qualitative risk assessment 9](#_Toc73534749)

[Figure 3‑3 - Quantified risk assessment 12](#_Toc73534750)

[Figure 3‑4 – Final quantified risk assessment 19](#_Toc73534751)

[Figure B‑0‑1 - Asymmetric cryptography 26](https://stichtingfontys.sharepoint.com/sites/ICTBusiness-Semester6697/Gedeelde%20documenten/PROF%20-%20Company%205/ATOS/ITA/ITA%20Rapport.docx#_Toc73534752)

[Figure B‑0‑2 - Signing 26](https://stichtingfontys.sharepoint.com/sites/ICTBusiness-Semester6697/Gedeelde%20documenten/PROF%20-%20Company%205/ATOS/ITA/ITA%20Rapport.docx#_Toc73534753)

# Management summary

This management summary gives a brief walkthrough of the IT audit report, for more detail go to the indicated chapters. The first chapter recaps the IT audit proposal, what is the IT audit object that is being advised upon and recapping what the research questions are. Then a scope is giving of which ISO27001 chapters are used in this document.

The first research question delves deeper into the risk assessment of the IT audit proposal, looking at the likelihood and impact. This risk assessment will be quantified, meaning that from a low, medium & high, a score from 1 through 5 will be assigned to likelihood and impact. The likelihood is based on how many times it would happen in a certain timespan. The impact is based on if the risk would violate one or multiple acceptance criteria.

The second research question focuses on the consequences that the risks have when they occur if the ISO 27001 framework is not applied. This chapter mainly focuses on the effect it will have on the quality aspects. The effect will be shown on the confidentiality, integrity, and availability as a direct effect of the occurrence of a risk and indirect consequences on the effectivity, efficiency, and verifiability.

The third and final research question adds the results of the previous two questions together. Combining these results with the scoped control measures of the ISO27001 framework to advise on mitigation steps for Atos, estimating how much the risk would be reduced. The conclusion of all these numbers and control measures can be found in figure 3-4.

Concluding with advice on which risk to treat and in what order, finishing this document with global advice.

# Introduction

This chapter gives a brief recap of the IT Audit Proposal. Chapter 1.1 describes the project; chapter 1.2 highlights the chosen ISO framework and which control measures are chosen in the scope. The last chapter 1.3 is about how this isn’t a normal audit but an advice audit for an information architecture design.

## Project description

Atos is developing a bridge between Siemens Teamcenter, SAP AIN, and the Internet of Things as a part of their ‘digital transformation’ portfolio, also called Industry4.0.

Designing a bridge between these three objects comes with hurdles, which can be tackled by using the right standard framework.

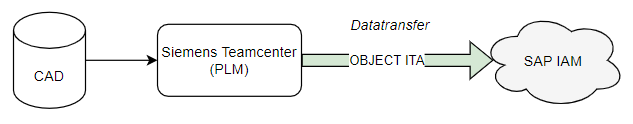
Atos has requested Elevate to focus on one part of the project; the bridge between Siemens Teamcenter and SAP AIN, where the object for the IT Audit is the data transfer between these two, as can be seen in figure 1-1.

Figure 1‑1 - Object

The IT Audit report will help Atos with solving two main problems:

1. Loss of intellectual property – When connecting Siemens Teamcenter to SAP, a new connection is established. This gives hackers a possible new entrance into the systems, which could result in the loss of intellectual property.
2. Wrong results – For example when an engineer receives the wrong information from the PLM system. This could result in an erroneous repair.

## Standard framework and scope

The ISO 27001 framework will be used to assess the security of the transferred data. According to (Panhalkar, 2020) seven annexes are related to data transfer in the ISO 27001. In ISO 27001 data transfer is referred to as ‘Information transfer’. The following annex of the ISO 27001 are applicable:

* A.10 Cryptography:
  + A.10.1.1 Policy on the use of cryptographic control measures;
  + A.10.1.2 Key management;
* A.13.2 Information transport:
  + A.13.2.1 Information Transfer Policies and Procedures;
  + A.13.2.2 Agreements on Information Transfer;
  + A.13.2.3 Electronic messages;
  + A.13.2.4 Confidentiality or Non-Disclosure Agreement;
* A.17.1.3 Verify, review, and evaluate information security continuity.

These annexes are chosen due to the relation to the audit object for this project and the related systems that are used.

**Relevance A.10 Cryptography**

This annex is relevant for the data transfer between Siemens Teamcenter and SAP AIN because the data needs to be secure. This can be achieved using encryption, signing, and key management and therefore this part needs to be assessed during the audit.

**Relevance A.13.2 Information transport**

This annex category will be part of the audit because the object of this audit is the data transfer between the two systems. Therefore, it is important to have control measures in place that make sure the transfer of the data is confidential and has several points to agree on in case of security of the transfer.

**Relevance A.17.1.3 Verify, review, and evaluate information security continuity**

This annex will also be included in the audit because is it important that the systems are continuously available to transfer data to keep the business continuity up. This needs to be verified, assessed, and evaluated continuously.

## Particularities project

The bridge between Siemens Teamcenter, SAP AIN, and the Internet of Things has yet to be made. This means that a conventional IT Audit is not possible. Instead of assessing the current state of the object, Atos has requested Elevate to research the ISO27001 framework and report on the most important aspects.

This report will then be used in the design stage of the project to make sure Atos suffices to the certification requirements.

# IT Audit

This chapter will show the research and process of the IT audit. In which the ISO27001 will be applied to help with formulating an advice for Atos. First, the research questions will be recapped. Then a short introduction of what ISMS is (This is a term that regularly comes back in ISO27001).

## Research Questions

### Main Question

How to use ISO27001 – Data Security for a secure information architecture, that allows for reliable data transfer between systems?

### Sub Questions

1. What are the risks for the designed information architecture?
2. What is the impact of the risks if the framework isn’t applied?
3. Advice on how to use the guidelines from the framework to assess data security?

## ISMS (Information Security Management System)

To receive an ISO framework certification, a working method needs to be adopted called the ISMS. An information security management system (ISMS) is a work method for the security of all confidential information within an organization. The ISMS is mandatory for a few internal/external audit activities (Axxemble, 2019). This demonstrates that your organization pays sufficient attention to information security.

The process approach of ISO27001 adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization’s ISMS. (INB, 2005)

An organization needs to identify and manage many activities to function effectively. Any activity using resources and managed to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the next process. (INB, 2005)

Using ISMS will guide the PDCA cycles (& operational planning). The ISMS anticipates (constantly changing) threats and opportunities from outside, responds to the needs from within the organization, and that correct measures are taken where necessary. This way the information security is efficient and up-to-date by using the ISMS in cooperation with PDCA.

**The PDCA cycle: Plan, Do, Check, Act**

Table 2‑1 - PDCA-cycle

|  |  |
| --- | --- |
| **Plan** | Mapping all potential intern and external threats/risks? Do the risks need to be transferred, dodged, or accepted? |
| **Do** | Realizing measures within the organization to control risks |
| **Check** | Check if the measures are efficient. Are the insufficient risks brought back? |
| **Act** | Respond to incidents to minimize impact and take corrective action to reduce the likelihood of new incidents. |

(Inergy, 2021)

# Results

All three research questions will be answered in this chapter.

## Sub-question 1: What are the risks for the designed information architecture?

In the proposal, a first risk assessment has been made, see figure 3 – 1. To make it more usable and unambiguous, the following changes will be made to the risk assessment:

* Quantify likelihood and impact – This makes the risk assessment more unambiguous.
* Deciding the impact score based on the violations of the acceptance criteria.
* Add gross and net likelihood and impact – multiplying likelihood x impact to score the gross risk

### Risk Analysis

Figure 3-1 shows a qualitative risk assessment based on high, medium, and low scores from the IT Audit Proposal. In this report, the risk assessment will be changed to a quantitative risk assessment.

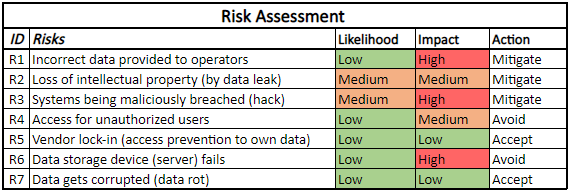


Figure 3‑1 - Qualitative risk assessment

### Quantified likelihood

[Appendix A](#_Appendix_A_–) gives a detailed thought process on how each likelihood is scored. The appendix gives an overview of what a likelihood score indicates. For example, a likelihood score of 1, would happen less than or once every 3 years. The results of Appendix A are included in figure 3-3 quantified risk assessment.

### Acceptance criteria & Impact analysis

Before deciding which action to take for each risk, the impact needs to be decided by the acceptance criteria. In the IT audit proposal, the following acceptance criteria were agreed upon with the client:

Table 3‑1 - Acceptance criteria

|  |  |  |
| --- | --- | --- |
| Acceptance Criteria | | |
| FC1 | Functional acceptance criteria | A user must be able to receive/extract product data from and to SAP AIN |
| FC2 | Functional acceptance criteria | A user must be able to receive/extract a guide of a machine on how to assemble from SAP AIN |
| NFC1 | Non-functional acceptance criteria | The data (file format) needs to be transferred in such a way that SAP AIN can import/read it |
| PC1 | Performance criteria | Siemens Teamcenter must be able to transfer the data within a timeframe of 5 minutes to SAP AIN |
| PC2 | Performance criteria | The servers have to be online from 6 a.m. till 8 p.m. for 7 days a week. This is based on certain customer and location time zone |

These acceptance criteria are used to define the gross impact of the risks. These scores will later be used to make a quantitative risk assessment.

**R1 - Incorrect data provided to operators – Impact 4**

The impact score is 4 (high) based on the fact that operators are skilled personnel that knows the machines they maintain and with the acceptance criteria’s it violates. However, SAP AIN recommending wrong spare parts could result in machine downtime. Looking at the acceptance criteria the following criteria are violated when this risk occurs. The violations are:

FC1: *“A user must be able to receive/extract product data from and to SAP AIN”*

NFC1: *“The data (file format) needs to be transferred in such a way that SAP AIN can import/read it”*

**R2 - Loss of intellectual property (by data leak) – Impact 4**

Intellectual property often gives organizations an advantage over competitors. A data leak could result in competitors catching up by using the intellectual property, resulting in a less advantageous position, which *could* cause a big impact over many years. Looking at the acceptance criteria this risk would violate:

FC2*: “A user must be able to receive/extract a guide of a machine on how to assemble from SAP AIN”*

A loss of intellectual property are the guides/blueprints of machines, this would violate functional criteria 2. With that in mind, R2 has been given an impact score of 4 (high).

**R3 - Systems being maliciously breached (hack) – Impact 5**

A malicious hack could result in systems being shut down and files being locked/deleted/stolen. Based on these the following acceptance criteria are violated:

FC1: *“A user must be able to receive/extract product data from and to SAP AIN”*

FC2: *“A user must be able to receive/extract a guide of a machine on how to assemble from SAP AIN”*

NFC1: *“The data (file format) needs to be transferred in such a way that SAP AIN can import/read it”*

If this risk would occur, then it would violate all functional and non-functional requirements. Because of this, the risk is given the highest score 5 (very high).

**R4 - Access for unauthorized users – Impact 2**

An employer may assume their employees won’t intentionally try to harm the organization. However, like already explained in ‘Loss of intellectual property (by data leak)’, employees could unintentionally leak data. This would then violate the following acceptance criteria:

NFC1: *“The data (file format) needs to be transferred in such a way that SAP AIN can import/read it”*

This risk would only violate the non-functional acceptance criteria, with that in mind the impact is scored with a 2 (low).

**R5 - Vendor lock-in (access prevention to own data) – Impact 5**

The impact of a vendor lock-in would be very high. An organization could lose access to their data (In case a vendor goes bankrupt and a switch to another vendor could not be done in time). Furthermore, a vendor lock-in could put an organization in a bad spot due to the leverage a vendor has at that moment (Possibly resulting in higher pricing for their products). This results in an impact score of 5 (very high), it would violate all acceptance criteria.

**R6 - Data storage device (server) fails – Impact 4**

The impact is scaled as 4 (high). As already explained, a failing hard drive would result in (partial) loss of the data that is on the hard drive. Organization critical files could be on these hard drives and loss could paralyze an organization. This would then violate the following:

FC1: *“A user must be able to receive/extract product data from and to SAP AIN”*

PC1: *“Siemens Teamcenter must be able to transfer the data within a timeframe of 5 minutes to SAP AIN”*

PC2: *“The servers have to be online from 6 a.m. till 8 p.m. for 7 days a week. This is based on certain customer and location time zone”*

**R7 - Data gets corrupted (data rot) – Impact 1**

The impact is scored on a 1 (very low), corrupted data will be re-requested to the system. It will use a backup to fill the request, in most cases, this will not cause a problem. It would violate one criteria:

PC1: *“Siemens Teamcenter must be able to transfer the data within a timeframe of 5 minutes to SAP AI.*

### Quantified risk assessment

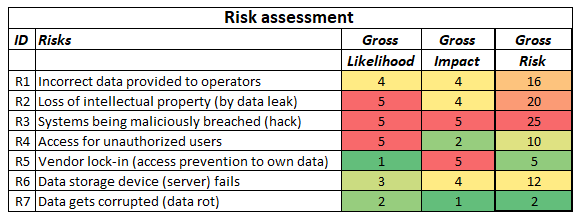


Figure 3‑3 - Quantified risk assessment

In [**Appendix A**](#_Appendix_A_–)the likelihood is quantified and in chapter [3.1.2 ‘Acceptance criteria & impact analysis](#_Acceptance_criteria_&)’ is the impact quantified. Both quantified scores are placed in figure 3-3. For each risk, the likelihood and impact score are multiplied by each other. As seen in figure 3-3 a color gradient overview is given that shows which risks are scored the highest. These risks can be reduced, advice for this will be given in later chapters. But first, the action is going to be defined, to advise what to do for each risk.

## Sub-question 2: What is the impact of the risks if the framework isn’t applied?

To show what the effect is of the risks if the framework is not applied, it needs to be clear what the impact of the risks is. This is determined in subparagraph 3.1.2 where the impact of the risks will be based on the acceptance criteria. This paragraph will focus on the quality aspects to see which risks from figure 3-1 influence certain quality aspects. The criteria and the aspects are both important for the final risk assessment to ensure a solid overview of the risks because this will also provide insights into the consequences a risk has if one occurs.

### Relation between risks and quality aspects

It is important to understand the effect of control measures on quality aspects. Chapter 1.2 briefly gives an overview of the chapters in ISO27001 which are most applicable to this project. From 3.2.1.1 onward, the effect on quality aspects is explained. The chapter headings also show what action needs to be taken to address the risks (E.g. mitigate, accept) and what chapter of the ISO27001 is applicable.

Below an enumeration of the quality aspects:

Table 3‑2 - Quality Aspect

|  |  |
| --- | --- |
| Quality aspect | Explanation |
| Confidentiality | The extent to which the object (Data and information-, technical- and process systems) is confidentially handled. This means that the system is designed with ‘privacy by design’ in mind to keep data and processes safe and that people will sign contracts stating they will keep data confidential. |
| Integrity | The extent to which the object (Data and information-, technical- and process systems) is following reality. Moreover, it is important to know that the data that is being used is released (Approved). |
| Availability | The extent to which an object is continuously available and the extent to which the data processing can continue undisturbed. |
| Effectivity | The extent to which an object complies with all requirements and goals set by the users and to what extent the object contributes to organizational goals. |
| Exclusivity | The extent to which only authorized personnel (or equipment) can make use of IT processes. |
| Verifiability | The extent to which it is possible to gain knowledge about the structuration (Documentation) and operation of an object. This aspect also includes the extent to which it is possible to establish that information processing is done in compliance with requirements to other quality aspects. |

#### R1 – Incorrect data provided to operators – Mitigate – A.13.2.1

**Quality aspect - Integrity**

If operators receive incorrect data from the system, this could result in a minor effect/change to a machine. However, the result could also be major in the form of a machine part that needs to be changed and due to the incorrect data, the wrong machine part will be replaced. This could result in malfunction of the machine.

#### R2 – Loss of intellectual property (by data leak) – Mitigate – A.13.2

**Quality aspect – Confidentiality**A data leak can occur by mistake or on purpose. Both can be done by human actions. Either way, the Atos’ data would be available for everyone. In both versions, this would result in a high level of failure in confidentiality towards clients.

#### R3 – Systems being maliciously breached (hack) – Mitigate – A.10.2.4

**Quality aspect - Confidentiality, Integrity & Availability**The influence of this risk on the quality aspects differs based on the hack. If the hack is meant to capture the data to withhold Atos from accessing their data, this would have a lot of effect on the availability of the data. However, in case of a hack that would open the data to the rest of the world, this would have a high impact on confidentiality. Integrity is about the correctness and fullness of the data. When a hack would remove some of the data this would affect the completeness of the data and thus on the integrity.

#### R4 – Access for unauthorized users – Mitigate – A.13.2.1

**Quality aspect - Confidentiality & Integrity**For this risk, it is the same as with the hack. An unauthorized user can alter the data by mistake or on purpose which, based on the intention, could results in reputational damage because confidentiality is compromised. Otherwise, the unauthorized access could, like the hack, result in incompleteness of the data.

#### R5 – Vendor lock-in (access prevention to own data) – Accept

**Quality aspect – Availability**A vendor lock-in could result in restrictions on access to an organization its data. This directly impacts availability and could result in operational damage.

#### R6 – Data storage device (server) fails – Transfer – A.17.1.3

**Quality aspect – Availability**A server failing means that it is no longer available to access. Since most, if not all, processes require a computer (connected to an organizations’ server), no access means that availability will be down. Availability that goes down means a direct effect on operations and thus created operational damage.

#### R7 – Data gets corrupted (data rot) – Accept

**Quality aspect – Integrity**Data getting corrupted can be the result of a lot of things, which is already explained in another chapter. Chances of it happening and damaging a system are low, but if data rot occurs beyond repair that would result in loss of integrity.

#### Effectivity, Exclusivity, and Verifiability

All the risks have been linked to quality aspects, which leaves effectivity, exclusivity, and verifiability.   
These three quality aspects are still affected by certain risks occurring, but more as a side effect than as a main.

For good measure, an example/explanation for the three above mentioned quality aspects and how they are affected:

* **Effectivity:**If any of the risks occur and other quality aspects are impacted, that means that the goals and requirements set by (end)users are not accomplished.
* **Exclusivity:**   
  Exclusivity is a requirement that is programmed into an application/solution. This Audit is about Data Security, which means that a compromise of the systemin inherently means the exclusivity is at risk.
* **Verifiability:**   
  Verifiability in basis means that the structure of everything is documented and that certain employees know about this and know the structure. However, a compromise of the system means that verifiability is possibly at risk.

## Sub-question 3: Advice on how to use the guidelines from the framework to assess data security?

In sub-question 3 the following point will be addressed:

* Add Atos control measures – based on the control measure of the ISO27001 documentation, advice control measures are given for the Atos company;
* The control measures stated in table 2 are connected to the risk assessment in figure 3-4;
* The gross risk likelihood and impact are before the control measures are applied, the net risk likelihood and impact are after control measures are applied.

### Control measures

These control measures are directly taken from the ISO27001, from each management objective that is mentioned in the scope of chapter 1.2 is in table 3-3. Each control measure will have a fourth column that addresses how Atos can apply these control measures for this project.

Some control measures refer to Appendix A – Control Measures, where a more in-depth explanation is added.

Table 3‑3 - ISO 27001: A.10: Cryptography

|  |  |  |  |
| --- | --- | --- | --- |
| **A.10 Cryptography** | | | |
| **A.10.1 Cryptographic control measures** | | | |
| Goal: Ensure correct and effective use of cryptography to protect confidentiality, authenticity  and/or integrity of information. | | | |
| A.10.1.1 | Policy on the use of cryptographic controls | *Control measures*  To protect information, a policy for the use of cryptographic controls should be developed and implemented. | *Atos Control measures*  Atos needs to set up a policy for using cryptographic controls. Using asymmetric encrypting data before transferring it between systems.  **See Annex B. ‘Encrypting’** |
| A.10.1.2 | Key management | *Control measures*  Regarding the use, protection of the lifetime of cryptographic keys, a policy must be developed and implemented throughout their lifecycle. | *Atos Control measures*  Master keys shall be updated once a year.  Key encrypting keys shall be updated twice a year.  **See Annex B. ‘Key Management’**  Inactive keys shall be destroyed (according to vendor guidelines).  **See Annex B. ‘Key Management’** |

Table 3‑4 - ISO 27001: A.13.2: Information transport

|  |  |  |  |
| --- | --- | --- | --- |
| **A.13 Communication security** | | | |
| **A.13.2 Information transport** | | | |
| Goal: Maintain security of information exchanged within an organization and with an external entity. | | | |
| A.13.2.1 | Information Transportation Policies and Procedures | *Control measures*  To protect the transport of information, which takes place through all types of communication facilities, formal policies, procedures, and controls for transport must be in place. | *Atos Control measures*  Mobile asset management will give operators digital data information, Atos will need to implement policies and procedures for this. |
| A.13.2.2 | Agreements about information transport | *Control measures*  Agreements must relate to the secure transport of business information between the organization and external parties. | *Atos Control measures*  Atos must have an exchange protocol with external parties and/or product owners (SAP & Siemens Teamcenter) to share data between systems. This ensures secure information transport. |
| A.13.2.3 | Electronic messages | *Control measures*  Information contained in electronic messages must be appropriately protected. | *Atos Control measures*  A data transfer should never contain more information than necessary for the purpose it serves.  Data transfers from Product Lifecycle Management Systems to ERP systems should always be encrypted. (Encrypting should be according to company standards, if there is no company standard, a company standard should be developed).  **See Annex B. ‘Encrypting’**  Data transfers from the IoT network to the ERP system need to be signed to be assured of data integrity.  **See Annex B. ‘Signing’** |
| A.13.2.4 | Confidentiality or Non-Disclosure Agreement | *Control measures*  Requirements for confidentiality or nondisclosure agreements that reflect the organization's needs for protecting information must be established, regularly reviewed, and documented | *Atos Control measures*  Having an NDA with SAP and Siemens about:   * The data; * The transfer of data; * Quarterly Review of the agreement(s). |

Table 3‑5 - ISO 27001: A.17.1: Information security continuity

|  |  |  |  |
| --- | --- | --- | --- |
| **A.17 Information security aspects of the business continuity** | | | |
| **A.17.1 Information security continuity** | | | |
| Goal: Information security continuity must be embedded in the business continuity management systems of the organization | | | |
| A.17.1.3 | Verify, review, and evaluate information security continuity. | *Control measures*  The organization shall regularly verify the controls identified and implemented for information security continuity to ensure that they are sound and effective during adverse situations. | *Atos Control measures*  Review previous control measures on a yearly or quarterly basis to maintain solid information security. |

### Quantitative risk assessment

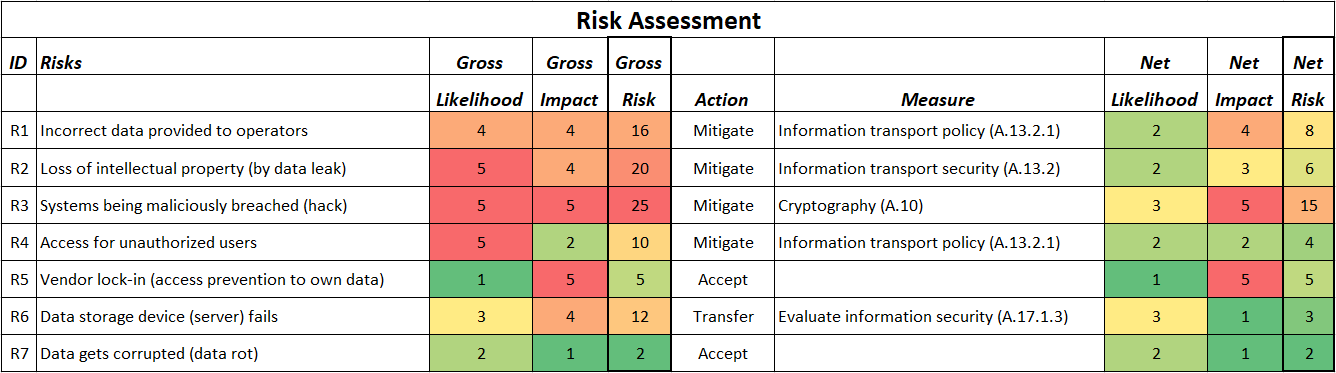


Figure 3‑4 – Final quantified risk assessment

Now that the impact is based on the acceptance criteria, the likelihood numbers need to have a basis as well. This is defined in table A-0-1 from Appendix A – Risk Analysis. Figure 3-4 shows each risk with an ID number, then what the risk entails, and the correlating score. Each likelihood and impact score is multiplied to get the risk score. This score indicates which risk to focus on first. The action column shows which following steps are advised to take. This can be mitigated, accept, avoid, or transfer. In the measure column, each input refers to chapter ‘3.3.1 Control measures’, as a way to reduce the likelihood and impact of each risk, that is chosen to be mitigated or transferred.

# 

# Conclusion

## Prioritization

From the seven risks that are most applicable to this project, there are a few that have the highest priority to implement:

* **R1 – Incorrect data provided to operators** – Since incorrect data is an operational risk, it is advisable to prioritize this risk. If the control measure ‘Information Transport Policy’ is not implemented, wrong data could render equipment and machinery useless/unavailable. Also, ‘Information Transport Policy’ is a measure that applies to R4, which means two risks are simultaneously tackled.
* **R2 - Loss of intellectual property (by data leak)** – Intellectual property is one of the most valuable assets of an organization. A data leak could mean competitors have access to this data which would mean that strategic advantages fade away. Since a lot of the data from machines, which might be considered intellectual property, is transferred from Siemens Teamcenter to SAP AIN, a control measure should be implemented to minimize the risk of data leaks.
* **R3 – Systems being maliciously breached (hack)** – Hackers become more and more active. Hackers could install malicious software on the organizations’ servers and could potentially also install ransomware. This is a big operational risk because it could shut down a company for days/weeks.

The other risks have a lower risk score. This doesn’t mean they shouldn’t be addressed but they also do not have the highest priority.

## Advice

This Audit report is an advice and should be treated as such. All control measures and advice on how to implement them are possible ways Atos can achieve better data security for their innovation project and get ISO27001 certified. This means that Atos is free to implement other measures how they see fit, and it also means that the advice will not necessarily mean ISO27001 certification will be possible if all stated control measures are implemented. The latter is dependent on how it is implemented in the final solution and if the solution will become exactly how it is described.

# Appendix

## Appendix A – Risk Analysis

In the IT audit proposal, a risk assessment was made with a likelihood/impact based on high, medium, and low scores. Each risk needs to be quantified, to give a clear determination of when something would happen and what the impact/damage would be. Based on that information the following table was created, for which each risk would be reassessed with a new score.

Table A-0‑1 - Meaning behind the likelihood risk scores

|  |  |
| --- | --- |
| **Score** | **Likelihood (Frequency)** |
| 1 – Very low | Less than or once every 3 years |
| 2 – Low | Once every 2 years |
| 3 – Medium | Once every year |
| 4 – High | Twice every year |
| 5 – Very high | More than twice every year |

On the next page, a more in-depth explanation can be found on the gross likelihood and gross impact. This is accompanied by control measures and the net results (with control measures acting as an explanation for the changed likelihood and impact).

**R1 - Incorrect data provided to operators**

Gross Likelihood: Wrong information could be provided because data stored in Siemens Teamcenter and SAP is incorrect. Furthermore, data corruption or faulty recommendations made by the system could result in incorrect data provided. The likelihood is scored a 4 which means that it will likely happen twice per year.

Gross Impact: The impact score is 4 (high) based on the fact that operators are skilled personnel that knows the machines they maintain and with the acceptance criteria’s it violates. However, SAP AIN recommending wrong spare parts could result in machine downtime. Looking at the acceptance criteria the following criteria are violated when this risk occurs. The violations are:

* FC1: “A user must be able to receive/extract product data from and to SAP AIN”
* NFC1: “The data (file format) needs to be transferred in such a way that SAP AIN can import/read it”

Control Measure: The following control measure should be used to **mitigate** this risk:

A.13.2.1. - Mobile asset management will give operators digital data information; Atos will need to implement policies and procedures for this. This ensures correct data is provided.

This results in a score of 2 for likelihood and 4 for impact (Impact does not change).

**R2 - Loss of intellectual property (by data leak)**

Gross Likelihood: The likelihood is scaled as very high (5) because a data leak could happen because of human error. Examples of a data leak are:

1. An employee could have unauthorized access to the data, which is considered to be a data leak.
2. An employee could intentionally leak data to other parties.
3. An employee could unintentionally leak data to other parties (as a result of inattention).

Gross Impact: Intellectual property often gives organizations an advantage over competitors. A data leak could result in competitors catching up by using the intellectual property, resulting in a less advantageous position, which could cause a big impact over many years. Looking at the acceptance criteria this risk would violate:

* FC2: “A user must be able to receive/extract a guide of a machine on how to assemble from SAP AIN”

A loss of intellectual property are the guides/blueprints of machines, this would violate functional criteria 2. With that in mind, R2 has been given an impact score of 4 (high).

Control Measure: The following control measures should be used to **mitigate** this risk:

* + - 1. A.13.2.1 - Mobile asset management will give operators digital data information; Atos will need to implement policies and procedures for this.
      2. A.13.2.2 - Atos must have an exchange protocol with external parties and/or product owners (SAP & Siemens Teamcenter) to share data between systems. This ensures secure information transport.
      3. A.13.2.3 - A data transfer should never contain more information than necessary for the purpose it serves.
      4. A.13.2.3 - Data transfers from Product Lifecycle Management Systems to ERP systems should always be encrypted. (Encrypting should be according to company standards, if there is no company standard, a company standard should be developed).
      5. A.13.2.3 - Data transfers from the IoT network to the ERP system need to be signed to be assured of data integrity.
      6. A.13.2.4 - Having an NDA with SAP and Siemens about:
         1. The data;
         2. The transfer of data;
         3. Quarterly Review of the agreement(s).

This results in a score of 2 for likelihood and 3 for impact, meaning both have gone down in severity.

**R3 - Systems being maliciously breached (hack)**

Gross Likelihood: If systems are not carefully secured for cyberattacks, the chances of it happening increase tremendously. This is because:

1. The number of hackers increases;
2. Hackers have more technology to cause more harm;
3. There is more malicious intent when hacking.

Because of these three reasons R3 has been given a likelihood score of 5 (very high).

Gross Impact: A malicious hack could result in systems being shut down and files being locked/deleted/stolen. Based on these the following acceptance criteria are violated:

* FC1: “A user must be able to receive/extract product data from and to SAP AIN”
* FC2: “A user must be able to receive/extract a guide of a machine on how to assemble from SAP AIN”
* NFC1: “The data (file format) needs to be transferred in such a way that SAP AIN can import/read it”

If this risk would occur, then it would violate all functional and non-functional requirements. Because of this, the risk is given the highest score 5 (very high).

Control Measure: The following control measures should be used to **mitigate** this risk:

1. A.10.1.1 - Atos needs to set up a policy for using cryptographic controls. Using asymmetric encrypting data before transferring it between systems.
2. A.10.1.2 - Master keys shall be updated once a year. Key encrypting keys shall be updated twice a year.
3. A.10.1.2 - Inactive keys shall be destroyed (according to vendor guidelines).

Cryptography lowers the likelihood of a malicious breach to a score of 3. The impact remains very high at 5.

**R4 - Access for unauthorized users**

Gross Likelihood: The likelihood is scaled as 5 (very high). This is because many organizations put too little time into checking employees’ authorizations.

Gross Impact: An employer may assume their employees won’t intentionally try to harm the organization. However, like already explained in ‘Loss of intellectual property (by data leak)’, employees could unintentionally leak data. This would then violate the following acceptance criteria:

* NFC1: “The data (file format) needs to be transferred in such a way that SAP AIN can import/read it”

This risk would only violate the non-functional acceptance criteria, with that in mind the impact is scored with a 2 (low).

Control Measure: The following control measure should be used to **mitigate** this risk:

A.13.2.1 - Mobile asset management will give operators digital data information; Atos will need to implement policies and procedures for this.

Having the right procedures lowers the likelihood from 5 (very high) to 2 (low). The impact remains on 2.

**R5 - Vendor lock-in (access prevention to own data)**

Gross Likelihood: A vendor lock-in is very unlikely to happen. There are multiple vendors for the software that this project uses. Also, other vendors/suppliers are likely to develop predictive maintenance software/applications, which would make a switch to other software simpler. Because of these reasons the likelihood of R5 is scored with a 3.

Gross Impact: The impact of a vendor lock-in would be very high. An organization could lose access to their data (In case a vendor goes bankrupt and a switch to another vendor could not be done in time). Furthermore, a vendor lock-in could put an organization in a bad spot due to the leverage a vendor has at that moment (Possibly resulting in higher pricing for their products). This results in an impact score of 5 (very high), it would violate all acceptance criteria. But the likelihood that this will ever happen is very low.

Control Measure: A vendor lock-in is unlikely to happen and is thus accepted. There are no control measures that should be put in place.

**R6 - Data storage device (server) fails**

Gross Likelihood: Without any measures, the likelihood of a data storage device fail is scaled as three. This means there is no backup in place and once the hard drive breaks down part of the data if not all data is lost. On average, the life of a hard drive is six years, with about 20% breaking down before the 5th year and another 30% in the 5th and 6th year. This results in a likelihood of 3.

Gross Impact: The impact is scaled as 4 (high). As already explained, a failing hard drive would result in (partial) loss of the data that is on the hard drive. Organization critical files could be on these hard drives and loss could paralyze an organization. This would then violate the following:

* FC1: “A user must be able to receive/extract product data from and to SAP AIN”
* PC1: “Siemens Teamcenter must be able to transfer the data within a timeframe of 5 minutes to SAP AIN”
* PC2: “The servers have to be online from 6 a.m. till 8 p.m. for 7 days a week. This is based on certain customer and location time zone”

Control Measure: The following control measure should be used to **transfer** this risk:

A.17.1.3 - Review previous control measures on a yearly or quarterly basis to maintain solid information security.

Furthermore, the risk is transferred to the cloud provider(s), which must ensure back-ups (Often also on multiple locations).

This results in a likelihood of 3 and an impact of 1. Note that the likelihood has not changed, since the lifespan of a hard drive remains the same. A backup however makes sure that a faulty hard drive has no impact on the day-to-day business of an organization.

**R7 - Data gets corrupted (data rot)**

Gross Likelihood: Data rots are primarily found by older hard drives, bitrot occurs when the electric current changes in a hard drive or SSD. At the current time bitrot doesn’t happen that often, hard drives and SSDs are better isolated for electric currencies. Because of these reasons, data rot is scored with a 2, so once every two years, it still occurs but not very often, there are also backups in place for cloud systems.

Gross Impact: The impact is scored on a 1 (very low), corrupted data will be re-requested to the system. It will use a backup to fill the request, in most cases, this will not cause a problem. It would violate one criteria:

* PC1: “Siemens Teamcenter must be able to transfer the data within a timeframe of 5 minutes to SAP AIN”

Control Measure: Data rot is very unlikely to happen. Even if it would happen, this would result in SAP requesting data and receiving faulty data, which often means (99% of cases) that data is unreadable. SAP will then put out another request, then most probably receiving the right data.

## Appendix B – Control Measures

### Encrypting and Signing

**Note: This Appendix describes one of many possibilities to secure data transfer between systems. If an organization has another solution in place, the implementing organization should look at compatibility and usability first.**

**Encrypting**

Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys (which may be known to others), and private keys (which may never be known by any except the owner). The generation of such key pairs depends on cryptographic algorithms which are based on mathematical problems termed one-way functions. Effective security requires keeping the private key private; the public key can be openly distributed without compromising security.

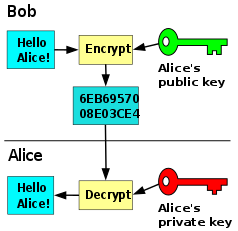
In such a system, any person can encrypt a message using the intended receiver's public key, but that encrypted message can only be decrypted with the receiver's private key. This allows, for instance, a server program to generate a cryptographic key intended for suitable symmetric-key cryptography, then to use a client's openly shared public key to encrypt that newly generated symmetric key. The server can then send this encrypted symmetric key over an insecure channel to the client; only the client can decrypt it using the client's private key (which pairs with the public key used by the server to encrypt the message). With the client and server both having the same symmetric key, they can safely use symmetric key encryption (likely much faster) to communicate over otherwise insecure channels. This scheme has the advantage of not having to manually pre-shared symmetric keys (a fundamentally difficult problem) while gaining the higher data throughput advantage of symmetric-key cryptography.

Figure B‑0‑1 - Asymmetric cryptography

**Signing**

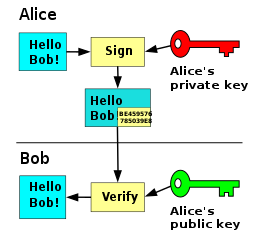
Not all data needs to be encrypted. For the data from IoT, integrity is a more important aspect (A hacker has little to no use for raw data from sensors). To be sure that the data is correct, signing can be used.

Figure B‑0‑2 - Signing

A sender can combine a message with a private key to create a short digital signature on the message. Anyone with the sender's corresponding public key can combine that message with a claimed digital signature; if the signature matches the message, the origin of the message is verified (i.e., it must have been made by the owner of the corresponding private key). (Contributors, 2021) (Velden, 2021)

**Key Management**

There are multiple ways a hacker could get his hands on a (private) key. For example, by brute force or by an internal leak. Because asymmetric cryptography is used, an obtained key does not necessarily mean a hacker can look through all data throughput of the past year. However, there is a slight possibility that the hacker does manage to get the necessary keys to keep intercepting data transfers.

To minimize the impact, keys should be managed properly:

* *Key Generation* **–** Master keys should be changed once a year. Key encrypting keys should be changed twice a year.
* *Key Destruction* – Keys that are no longer used (For example sensors that have reached their end-of-life and are replaced still have a key in the system) should be deleted as soon as possible.
* Key Compromise – If keys are (suspected) compromised an organization will have to identify the leak, fix the leak, and replace the keys as soon as possible. Also deleting the old, compromised keys should be done as soon as possible.
* *Key Recovery* – A recovery agent must be implemented so that decryption always remains possible. This could be the case if malicious software deletes (part of) the decrypting keys in the main system. If there is no recovery agent in place, deletion of decrypting keys could render data useless. (CalPoly, sd)

# Bibliography

Axxemble. (2019, 07 22). *Wat is een ISMS en waarom (en wanneer) moet u dit gebruiken?* Retrieved from Blog.axxemble: https://blog.axxemble.nl/waarom-isms#:~:text=De%20ISO%2027001%20certificering%20gaat,ofwel%20Information%20Security%20Management%20System.

CalPoly. (n.d.). *IT Security: Encryption Methods and Recommended Practices*. Retrieved from CalPoly: https://security.calpoly.edu/content/encryption-practices

Contributors, W. (2021, April 24). *Public-key cryptography*. Retrieved from Wikipedia: https://en.m.wikipedia.org/wiki/Public-key\_cryptography

INB. (2005, 11 01). *Information technology – Security techniques – Information security management systems – Requirements.* Winterthur: SN. Retrieved from SN.

Inergy. (2021, 03 02). *PDCA-cyclus voor informatiebeveiliging en privacy*. Retrieved from Inergy.nl: https://inergy.nl/blog/pdca-cyclus-voor-informatiebeveiliging-en-privacy/

Panhalkar, T. (2020, Juli 13). *ISO 27001 Annex : A.13.2 Information Transfer*. Retrieved from Infosavvy website: https://info-savvy.com/iso-27001-annex-a-13-2-information-transfer/

Velden, T. v. (2021, Mei 13). Bsc Cybersecurity. (M. Post, Interviewer)