Tampere University of Applied Sciences

IT Security integration after acquisition - case Sandvik and DSI Underground

Joonas Putaansuu

BACHELOR'S THESIS
May 2022

ICT Engineering
Telecommunication and Networks

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in ICT Engineering
Telecommunication and Networks

PUTAANSUU, JOONAS:
IT Security Integration After Acquisition -
Case Sandvik and DSI Underground

Bachelor's thesis 46 pages, appendices 6 pages
May 2022

This thesis work was commissioned by Sandvik Mining and Construction Oy concentrating in their IT integration process after acquiring a company called DSI Underground. Sandvik has a growth strategy that includes acquisitions, and the aim of this thesis work was to explore the possible problem areas in the integration process following an acquisition.

There are many dependencies between modern day IT systems and integrating two IT infrastructures together is a challenge. The goal of this study was to find out how to achieve as seamless integration process as possible.

Some of the current processes in use at Sandvik were charted by going through internal policies, procedures and guidelines regarding M&A, IT and IT security. Sandvik internal M&A experts were also consulted about the current and possible optimal future processes used for IT integration.

As a conclusion, this thesis lays out some steps to follow in order to get the IT integration process to flow smoothly and to avoid the problems that commonly arise. Sandvik has done many acquisitions over the years and improved the integration process, so there was no need to remake the whole process or make any drastic changes.

Key words: it integration, it security, acquisitions

CONTENTS

GLOSSARY

AD	Active Directory
AAD	Azure Active Directory
BA	Business Area
BIA	Business Impact Analysis
CAIQ	Consensus Assessment Initiative Questionnaire
CMDB	Configuration Management Database
EHS	Environment, Health and Safety
GDPR	General Data protection Regulation
HR	Human Resources
ITIL	Information Technology infrastructure Library
M&A	Mergers and Acquisitions
SAAS	Software as a Service
SIEM	Security Information and Event management
SITS	Sandvik Information and Technology Services
SMR	Sandvik Mining and Rock Solutions
SNC	Sandvik Network Client
VDR	Virtual Data Room

1 INTRODUCTION

On a global level, multinational enterprises often acquire their smaller competitors or merge with equally large companies. In multinational enterprise level, these acquisitions are very broad and complicated subject. After the transaction there is a need to decide, how the acquired company, will be integrated to the acquiring company. Will the newly acquired company stay as a completely stand-alone company or will there be full integration, where the new acquisition is to be consolidated in the buying corporation, or possibly something in between.

In multinational enterprise level, IT systems are very complex and there are lot of dependencies. Both companies could very well have thousands of servers and applications in use around the world. Companies can have a diverse array of applications and system to support their business and integration decisions are needed for all of them.

Sandvik AB is a multinational industrial conglomerate, that acquired another multinational underground mining and tunnelling company DSI Underground in 2021. From this acquisition started a long integration work, with a goal of consolidating DSI in to Sandvik where it will become its own business division.

While that is the goal of the integration process, the goal of this thesis work is to follow and chart the integration process in the IT security area. This thesis tries to find those problems that arise from the dependencies that are built into the IT infrastructure. Goal is to chart the right sequence for IT system integrations, as many of these systems use the data from another solutions. If the data is missing in the first steps the problem will compound later in the process.

2 ACQUISITION

In this section of the thesis work, the overview of different phases in the acquisition process is laid out. This will show what steps there are in this whole process even before any integration is planned or implemented. As this thesis works scope is IT Security integration these acquisition chapters will be brief.

2.1 Before transaction

The pre-transaction is defined as: “From identified target with clear intention to buy or sell until an indicative bid has been placed or letter of intent signed.” (Sandvik Acquisitions and Divestments Policy 2021).

There is a lot happening in the M&A process before the actual transaction. Sandvik has an acquisition strategy that dictates how the company seeks to find acquisition targets. This is an ongoing screening process for the said targets. When a possible target is identified, that triggers the process.

In the pre-transaction phase, there is an appropriate project management and governance structure established. This usually has a Steering committee, business owner to whom the acquired business will report and project leader to handle the day-to-day management.

Planning the project in this stage is crucial and it is also recommended to keep a log of people who are informed of the project. This logbook is because at this stage the project usually is still confidential until signing and announcement.

At the pre-transaction phase there is also a financing assessment to assess the acquisitions impact on the Sandvik groups credit rating. Initial risk management process is also done at this stage. The goal of risk management process is to identify the possible risks associated with the acquisition. This is done using the Sandvik Enter Price Management model. Risks to be identified include valuation risk that can result in a too high valuation for the acquisition target, business risk that will mitigate the whole case for the acquisition, compliance and reputational

risks stemming from legal or environmental, social and governance aspects or other risks. (Sandvik M&A Procedure 2021)

2.2 Transaction phase

At the transaction phase the true assessment can start. At this stage the data room opens. This is usually a virtual data room (VDR) where Sandvik can provide questions to the acquisition target company, and they will provide answers to those questions. Here is where the target company can provide statement, contracts, licensing information and overall information on their company infrastructure and assets.

At the transaction phase there is further financial analysis, more granular risk assessment, tax and legal assessment here the transaction negotiation documents are exchanged. At this stage the formation of integration plans will start with day 1 and day 100 plans.

In transaction phase the business case for the acquisition is assessed. This includes identified up- and downsides in targets business plan, possible synergies from integration in to Sandvik group and takes into consideration the transaction and integration cost. Also, financing and legal structures are assessed and set up at this phase.

In transaction phase there is access to more financial information, so more in-depth valuation of the target company is performed. In this phase the compliance and competition law assessments are performed and plans about brands and trademarks are made.

2.2.1 Integration planning

As per Sandvik M&A procedure, an integration plan is to be prepared for all acquisitions (Figure 1). Transaction phase Is where making a detailed integration plan starts and that plan is monitored and modified until the transaction is completed. After the transaction is completed the integration process detailed in

the plan starts on day 1. Plan will be finalized during the first 100 days after the transaction is complete.

As early as possible in the project, the wanted integration level should be decided. The desired depth of integration will guide decision making throughout the whole process. There are usually few common patterns for this. The aim could be for just a minimum integration, that basically means no integration. Minimum integration means that some basic security controls are required from the acquired company, but there is no connections to the buying company IT infrastructure. Second options are infrastructure and collaboration integration. This means that the acquired company infrastructure is connected and use the buying company identity and access management, network client SNC and e-mail and SharePoint. The third option is full IT infrastructure integration. In this option the acquired company starts using all or some of the business systems used in the buying company and this way will become part of the acquiring company.

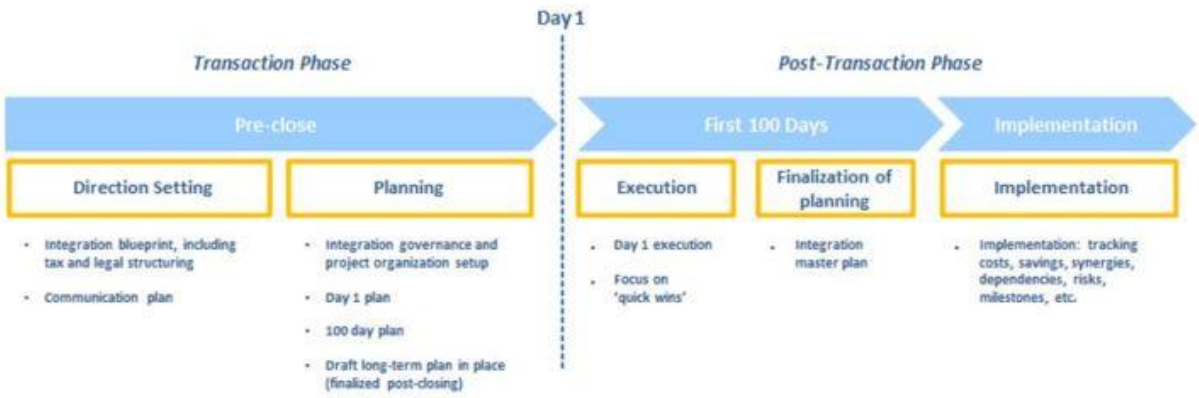

FIGURE 1. Integration planning and implementation. (Sandvik M&A Procedure 2021)

2.2.2 Due diligence

In transaction phase when the data room opens the due diligence process starts. Due diligence is an investigation to the target company. At Sandvik side there are a big due diligence team formed. This team will be responsible for the due

diligence and includes people from multiple areas in the business. In the due diligence process time is of the essence, as there might be other possible companies competing for the same acquisition.

Due diligence scope is vast and has many areas of interest. It aims to identify possible risks in the target company, confirm the material facts and assumptions and validate the investment case. This also includes quantifying the full potential of the acquisition in Sandvik ownership. Due diligence also aims to provide input to the integration plan. (Sandvik M&A Procedure 2021)

The scope of due diligence tries to cover all possible areas of risk in business. These include Finance and tax, EHS, Operations, IT, HR, Legal and Sustainability. (Sandvik M&A Procedure 2021). In this thesis, the scope is only the IT stream, so that is where this work will focus.

2.2.3 Due diligence IT stream

There is a M&A project due diligence team formed for IT. This team doesn't always encompass all the same people because it depends what part of Sandvik group is acquiring the target. Although there are some key players in the Sandvik group who are usually part of this team.

This team utilizes the virtual data room where they provide questions for the target company to answer. This is a digital platform where both parties can input their material. Team can also have expert call with the target company chief information officer or IT manager.

When the team poses questions to the target company IT department it is desirable that they provide some documents relating to their answers so that the facts can be verified.

The goal of the due diligence team is to investigate the target company IT infrastructure. Team aims to get an understanding of the existing IT landscape, identify risk areas and liabilities to manage in the transaction.

The initial focus of the due diligence is on compliance in security, relevant licenses and agreements. Due diligence team also tries to identify potential synergies. Here it is important to understand the integration ambition from business side and the implications for the future integration. Here is also where the initial assessment for one-off integration cost and the impact on IT operational costs after the integration is made.

Due diligence process scope includes the whole IT landscape. Team maps out the target company IT infrastructure and operations. Team tries to identify all the hardware and software assets, licenses, service provider agreements, outsourcing agreements and get a sense of the overall architecture. This includes targets hosting environments in datacenters and cloud services, disaster recovery plans and architecture, end user computing and network architecture.

Due diligence also aims to assess the targets IT governance structure, IT policy and procedures, this includes targets IT security policy and procedures, identity and access management and what IT security tools the target has in use.

Team aims to investigate any possible risks relating to IT. Where is the solutions and software that the target is using sourced, is the related licensing handled properly and how has the architecture been set up.

Although IT stream is usually not the showstopper in the acquisition process it is important for finding out and mitigating possible risks in IT. IT stream in due diligence feeds input to the integration plan so that the right steps can be taken from day 1 after the transaction.

IT due diligence stream will produce a due diligence report where the findings have been listed. The findings in the report give insight to the target company IT infrastructure and used solutions. This report gives the basis for integration work and recommends what controls need to be implemented on the security side. The report also gives an estimation of costs associated with getting the acquired company compliant and integrated to appropriate level.

3 INTEGRATION GOALS AND PLAN

This chapter will explain the goals of the whole integration process. How the planning starts and what different options there are for integrations and how these are used in Sandvik for new acquisitions.

3.1 Integration goals

Sandvik group strategy dictates that the group is to grow their business through acquisitions of other companies. After the target company has been identified the acquisition process will start. As outlined in this thesis, there are lot of steps in the process along the pre-transaction and transaction phases. Due diligence is a very important process to investigate the acquisition target thoroughly. There is a valid need to know as much as possible about the target company before transaction so that the acquisition can be justified from business reasons. After the transaction has gone through the integration really starts.

Usually in M&A activities, the overall reason for the acquisition is to grow the business. This means that possible reasons for acquisitions includes access to new markets, growing market share, bring with it new products or other intellectual property or such big synergy advantages, that it will help bring down production costs.

Goal of the integration process is to finalize the acquisition and achieve these benefits for the business. The integration process must be planned ahead, by defining the desired business goals for the acquisitions and forming the integration process around those goals. Integration process strives for a as smooth integration of the acquired company as possible, to the existing systems and services of the company doing the acquisition. For the acquired company to be able to bring value, it must be able to continue its business without interruptions. This is the reason that the integration process should be done smoothly and be planned well ahead of the day 1 after the transaction.

3.2 Integration plan

The integration plan starts with a valid business case for the acquisition. There is a need to define what business advantages are pursued with the acquisition. After the desired business advantages have been identified, there needs to be an examination, on what depth of integration will best serve those goals. There is also a need to know the future plans for the acquired business. Even if, at the current stage less integration would be enough, those future plans will dictate the integration depth needed.

Depending on the integration ambition, at the initial phase, there should be plans for a full security audit to verify facts about the acquisitions IT security. Possible site visits, creating company codes in all IT administrative systems, user account creation and network connectivity.

At the beginning, ambition level for the integration has to be decided. In M&A there are usually 3 levels of integration that is used for acquisitions. There needs to be a thorough assessment of the acquisition's future place in the acquiring company, so the correct integration level can be chosen.

3.2.1 Integration option 1 – Full integration

The first and most in depth integration commonly used on M&A, is full integration. Even though this is option one, it does not mean that his is the most desired, best or even most common option.

In Sandvik, full integration means that there is full onboarding of acquired company systems to Sandvik common IT services and also integration with given business areas processes and systems. (Integration options in acquisitions PowerPoint, 2019)

In IT, the full integration term is often used to describe what is actually a full IT infrastructure integration, but this does not state anything about how business areas conduct their business integration.

The full IT infrastructure integration means that the acquired company will start to use all the Sandvik processes, services, solutions and delivery organizations. This will bring the acquired company to be fully part of Sandvik. The acquired company will be integral part of the Sandvik business area it belongs to and fully utilize all or most of Sandvik business processes and tools. This also enables full access to all Sandvik internal systems and information for the acquired company. This way the acquisition will automatically become compliant to Sandvik policies.

There are also possible down sides to the full IT infrastructure integration. It could possibly require, that the acquired company abandons its old ways and accepts and implements Sandvik business areas business systems and tools. There is not as much freedom of choice anymore for what tools they want to use and where they will source the delivery for their services.

There can be a scale for what processes and systems will be adopted straightaway and what will come on a later stage. There might be long running contracts for different services from many outside vendors that will have to be renegotiated or used for the contract period, before starting to use Sandvik systems.

The full IT infrastructure integration is the option that will eventually on some date be implemented on DSI Underground as it will become a whole new business division inside the Sandvik Mining and Rock solutions business area.

3.2.2 Integration option 2 – Infrastructure integration

Then there is the second IT integration option that is IT infrastructure integration. This is a sort of middle of the road integration option commonly used in M&A. In Sandvik, this is defined as onboarding the Sandvik common IT infrastructure services to support collaboration, enable the use of Sandvik systems and prepare for further business integration as and when required. (Integration options in acquisitions PowerPoint, 2019).

This means that the business systems and old business processes that the acquired company is using are kept as is, at least in the beginning.

This approach enables access to all the acquiring company internal systems and information. Helps the acquired company to be compliant to required policies, procedures and onboard all the mandatory IT systems, services and controls, hence future proofing the acquired company IT infrastructure. In this option the acquired company infrastructure is connected to the buying company and standard structure for identity and access management is used. This option includes collaboration tools such as e-mail and SharePoint between the two companies.

This is also the bedrock for deeper future business integration. In this option the acquired company still retains some freedom in choosing the business systems they want to use.

3.2.3 Integration option 3 – Minimum IT integration

The third IT integration option is minimum integration. This is the option for maximum choices but as the name implies the minimum true integration. There is a scale to this option also. Minimum integration can be done as a true minimum which means that there will be the bare minimum integration to achieve compliance to necessary policies. This can be also called no integration as the acquired company will retain the right to choose the systems, services, service delivery organisations and solutions they are using.

On the other end of the scale this integration option may include many of the options that are encompassed in option 2. In this option the integration is tailor built for the needs of the acquired company and to the integration ambition from the acquiring company.

In integration option 2, the acquired company’s existing infrastructure can be, to some extent, operated as a stand-alone infrastructure system outside of the acquiring company infrastructure.

Option 3 also has the most down sides. This option means that the acquired company has to fund, build and manage their systems, services and solutions so that they are kept compliant to the mandatory requirements in acquiring company policies. As this process is always done as a one-off case, there is a true risk of building very confusing and complex IT security architecture. This option will also not be the best option if there is a need to reach IT resources or information hosted inside the acquiring company's internal network.

At minimum, this option needs that the acquired company employees are added to buying company HR system and user accounts are created for those employees. As a consequence, these employees might have user accounts in both companies, at least in the interim but these dual accounts could also be long-term depending on the chosen integration depth.

Depending on the acquiring company's policies and procedures, there might also be a need to implement appropriate anti-malware protection, SIEM logging, documenting of assets to asset management database and vulnerability scanning on those assets.

4 POLICY

Sandvik is a big multinational enterprise with long and rich history. Company this size must have a well thought out governance frameworks that will guide how company operates and how it is run. In this section of the thesis work I will go through some of Sandvik policies and procedures that have a governing role in acquisitions and integration process.

4.1 Governing way of working

In a big multinational enterprise, there should be a governance framework that encompasses all the policies and procedures for guiding way of working in that company. In Sandvik there is a governance framework called Sandvik Way (Figure 2). This is a collection of documents that guide working in Sandvik.

FIGURE 2. Sandvik Way description, Sandvik intranet, 2022

From Sandvik Way framework, documents to guide daily work in Sandvik, can be found. Here are roles and responsibilities that apply to Sandvik and guides how things should be done to live up to Sandvik core values. These core values in Sandvik are innovation, customer focus, fair play, and passion to win.

For the scope of this thesis work most important documents in Sandvik way are the ones regarding Compliance and risk. Here are the policies and procedures that dictate how everything should be done in Sandvik.

4.2 Sandvik policies regarding M&A

In Sandvik Way there is Sandvik Acquisitions and divestments policy. This is a policy to help manage M&A project appropriately and help manage the several types of risks entailed in these projects.

The purpose of this policy is to outline the requirements for the entire M&A process. The aim is to ensure that all M&A project at all levels within Sandvik Group are based on informed decisions, approved by the appropriate delegated authority with a reasonable risk balance and well executed.
(Sandvik Acquisitions and Divestments policy, 2021)

In Sandvik Way there is also Sandvik M&A Procedure part 1 – Acquisitions. It is a complimentary document to the Acquisitions and Divestments policy and is a framework for large transactions. It gives additional information and instructions for how to apply the mandatory definitions, principles and processes outlined in the policy. The M&A procedure should not be considered as a manual for how to execute all aspects of M&A projects.
(Sandvik M&A Procedure Part 1 – Acquisitions, 2021)

From Sandvik Way also comes the Sandvik M&A Procedure part 3 – The Sandvik Way Implementation. This procedure applies to all acquisitions within Sandvik Group and is intended to facilitate integration planning by providing an overview of The Sandvik Way, including guidance on timeline for implementation.
(Sandvik M&A Procedure Part 3 – The Sandvik Way Implementation, 2021)

These are the central policies and procedures used in Sandvik for managing acquisitions. From these comes the requirement for compliance and timelines to be fulfilled.

4.2.1 Sandvik policies and procedures for IT security

In Sandvik Way there are multiple documents for guiding IT. From these the IT Policy and IT Security Policy are the two policies that jointly form the overall governance of IT at Sandvik.

Sandvik IT Policy purpose is to provide a framework to ensure decisions with wide-ranging consequences due to sharing of software, infrastructure and information can be made transparently by each business unit, allowing the whole of Sandvik to reach overall growth and profitability targets while managing risks and capturing opportunities. IT Policy strives to ensure that IT across the organization is used in compliance with laws, regulations and the Sandvik Way.
(Sandvik IT Policy, 2020)

IT Security is a prerequisite to ensure digital trust for all IT assets and solutions within Sandvik. IT Security Policy contributes to the growth of business capability, competitiveness and sustainability by mitigating IT security threats to the Sandvik business. The purpose of IT Security policy is to stipulate requirements and obligations related to IT security at Sandvik.
(Sandvik IT Security Policy, 2020)

4.3 Acquired company policies

In mergers and acquisitions the acquired company will probably have its own policies and procedures regarding the way of working in that company. It is always good if these documents are provided in the due diligence phase in the virtual data room. From here Sandvik due diligence teams can get access to these documents and get an overview of how the target company conducts its business.

It is not enough to get access to these policy documents and take them at face value. It is always good practice to try to verify that these policies and procedures are truly followed in the target company. Here it is always best if the target

company can provide certificates from third party that has audited their processes.

It is also important for Sandvik teams to keep an open mind when going through these documents, because there might always be something to learn from acquired companies. Just because the buying company might be bigger and older it does not mean, that their way of handling IT infrastructure is superior. Still the main point is, to gather information on the target company infrastructure, for it is needed when planning the integration process.

If the acquired company has an IT security policy, it should state the IT security controls required in that company. These could include their network security controls, identity and access management policy, malware protection and vulnerability detection. Although, even if the acquired company policy is on a good standard and states the required controls, there is still a need to verify that the policy is truly followed.

If it is possible to conclude from these policy and procedure documents that the target company IT infrastructure security is up to the same or close to the same standards that Sandvik requires on Sandvik IT, then the integration will possibly be easier.

4.3.1 State of Acquisitions IT security

Sandvik has IT security policy and IT security procedure that dictate the way IT security is handled. The state of acquisitions IT security need to be assessed thoroughly and compare it to Sandvik stated requirements.

Solutions used in the acquired company don’t have to be exactly the same ones that are used in Sandvik, if they are assessed to fulfil the requirements. It is possible to keep using the original security solutions in the acquired company till their possible contract periods run out, without the need to rush to replace them. If there are different security solutions in use, but they are assessed to be up to required standards, then this will not be an obstacle to the integration.

It might be, that the easiest way is to change the security solutions and service providers to be the same what is already in use at the acquiring company. This way managing security controls and monitoring is easier to implement and can stay up to date, with the state of the acquisition's infrastructure.

There is also a need to chart out, what solutions are different from those used in the acquiring company, and that will possibly stay in use at the acquired company. After this charting, there needs to be a risk level assessment of those solutions and security controls implemented on them. If these security controls aren't enough to fulfil the acquiring company requirements, some additional controls might have to be implemented. This possible requirement of additional controls depends on the risk appetite of the business unit where the acquired company is to be integrated. More risk averse business units will demand more additional risk controls while some others might not.

5 IDENTITY

In this part of thesis work I will go through a concept of digital identity. Digital identity can have many forms but here it is meant to represent digital identities as they are used in Sandvik. Sandvik has internal governance policies and procedures that dictate what digital identities mean in the company, in acquisitions and in the integration process.

5.1 Digital Identity

Sandvik has a HR system for managing digital identities. In Sandvik Way there is Sandvik Identity and Access Management Procedure. In this procedure it is stated that, all digital identities shall be linked to natural living person. Either by direct relationship or by ownership. Purpose of this is to allow traceability of access to information and systems. (Sandvik Identity and Access Management Procedure, 2018)

All granting of access shall follow a documented segregation of duty principle where there is a segregation between the one who will receive an access and the one approving the access. All accounts shall have a documented purpose and have a responsible or be owned by a Sandvik employee to ensure accountability within Sandvik Group. All access shall be covered by a documented and frequently reoccurring revalidation process to ensure they are appropriate, necessary, valid and related to a documented business process. (Sandvik Identity and Access Management Procedure, 2018)

The above is picked from Sandvik procedure. This is what is required from the acquired company. These controls must be implemented by already existing policy or procedure, or this needs to be implemented in the integration process. Whatever the implementation stage for these controls, this is expected of the newly acquired company for there to be trust in the IT infrastructure. This is the way Sandvik governs digital identities, but other companies might do this differently.

5.1.1 Employee ID

In mergers and acquisitions, the employees from the acquired company will need to be documented to the HR system for them to have a digital identity. This is not mandatory in all companies, but if those new employees of the acquired company, don't have digital identities, the integration process will be lot harder. As stated above, Sandvik Way demands that people with contractual relationship to Sandvik must have a digital identity. In Sandvik, this is mandatory within 24 months after closing. This is usually required in almost all companies in one way or another. From HR system these employees will get their employee ID that is unique to them and will be how they are identified in the company.

In modern IT systems there are a huge number of dependencies. This basically means that if one piece of information is missing, the whole stack of systems doesn't work as intended.

HR system and digital identity are one of the most important and one of the earliest steps in the integration process. At the beginning of integration, key employees from the acquired company, should be documented to the HR system for them to get digital identities and employee IDs. In the HR system that Sandvik uses, there are a lot of different tools for reporting, payroll and training. In the beginning, there is no need to implement this whole range of tools to these new employees from the acquired company, but the basic information from them is required, so that digital identities can be achieved and used in other systems.

5.1.2 Accounts

By documenting new employees to the HR system and getting them their employee IDs**,** the integration process can be started. After the key employees have got their digital identities, they can have user accounts and access rights associated with these accounts. When these key employees from the acquired company get accounts, they can access basic collaboration tools like email and SharePoint.

Once these employees are in the system and have access to the basic collaboration tools, they can start working on internal company trainings and learning the systems that are in use. For example, In Sandvik there are some internal trainings that are mandatory to every employee, like Anti-Bribery and Corruption training and the Code of Conduct training. At this stage in Sandvik, these employees get access to the policies and procedures in Sandvik Way and can get started on learning and implementing them.

As an example of problems that arise if this digital identity is not obtained. In Sandvik, without getting the digital identity and user accounts, these new employees aren't known in Sandvik systems. This means that they can't be registered to have any roles, they can't be documented in configuration management database groups, or they can't even create tickets to IT support from the problems they encounter.

So, in Sandvik case, digital identities from HR system, employee ID's and user accounts are truly one of the most important first steps in the integration process. It is a lot of work to fill in new employee information to the system, but there is no need to get every employee in there straight away but only some key employees.

When these key employees get their digital identities, they can assume roles in different systems and get access to collaboration tools like email. With digital identity, these employees also get access to acquiring company policies, procedures and trainings so they can start implementing these at the acquired company.

6 ACCESS MANAGEMENT

in this section, this thesis will go through access management and Active Directory. Access management is the other side of digital identity as there always is who and what access. Access management also has a big role in acquisitions and integrations as it is the way to give access to new employees to existing resources.

6.1 Active Directory

“Active Directory is a common repository for information about objects that reside on the network, such as users and groups, computers and printers and applications and files” (Allen & Lowe-Norris, 2003,2).

So Active Directory is a directory services software, created by Microsoft, where information about an organisation can be stored and managed. Active Directory also has authentication and access control built in. This means that the users stored in AD, can be authenticated when they sign in, and administrators can manage their access rights centrally from one place. (Microsoft documentation, Active Directory Domain Services, 2022).

Information about company assets is stored in Active Directory, this information could be users, user groups, computers more. AD is also where administrators assign access rights of different kind. For example, there might be a group that has access permission to certain application, if user is then added to this group, they will automatically get access to that application.

6.1.1 Active Directory structure

Active Directory is used for authentication and access management in both Sandvik and DSI Underground. This means that if the goal is for employees from DSI underground to get access to Sandvik systems and services, these two Active Directories need to be integrated.

Active Directory is the authentication and access rights management tool. This means that it is crucial for IT security. Someone might describe it as keys to the kingdom. For this reason, there needs to be careful consideration, when adding new users or service principals to Active Directory.

Active Directory has a hierarchical structure similar to filesystem, where data is stored as objects. (Allen & Lowe-Norris, 2003,10). Mentioned above are users, printers and service principals, these are examples of objects stored in Active Directory.

Active Directory has a logical structure that consist of organization units, domains, trees and forests. Organizational units are logical container objects, where user, group and security policy objects can be added and managed (Microsoft documentation, What are Domains and Forests?, 2014).

These Organizational units that hold for example users, can then be arranged into domains like Sandvik.com. These domains are again logical containers that can hold many Organizational units and that way many user objects. Big organizations can have many domains and subdomains for different business areas like for example marketing.sandvik.com. These domains are then logically arranged in domains and subdomains that is called a tree (Figure 3). Finally, all these domain trees form an AD forest. (Allen & Lowe-Norris, 2003,11)

Below is an example of domain tree

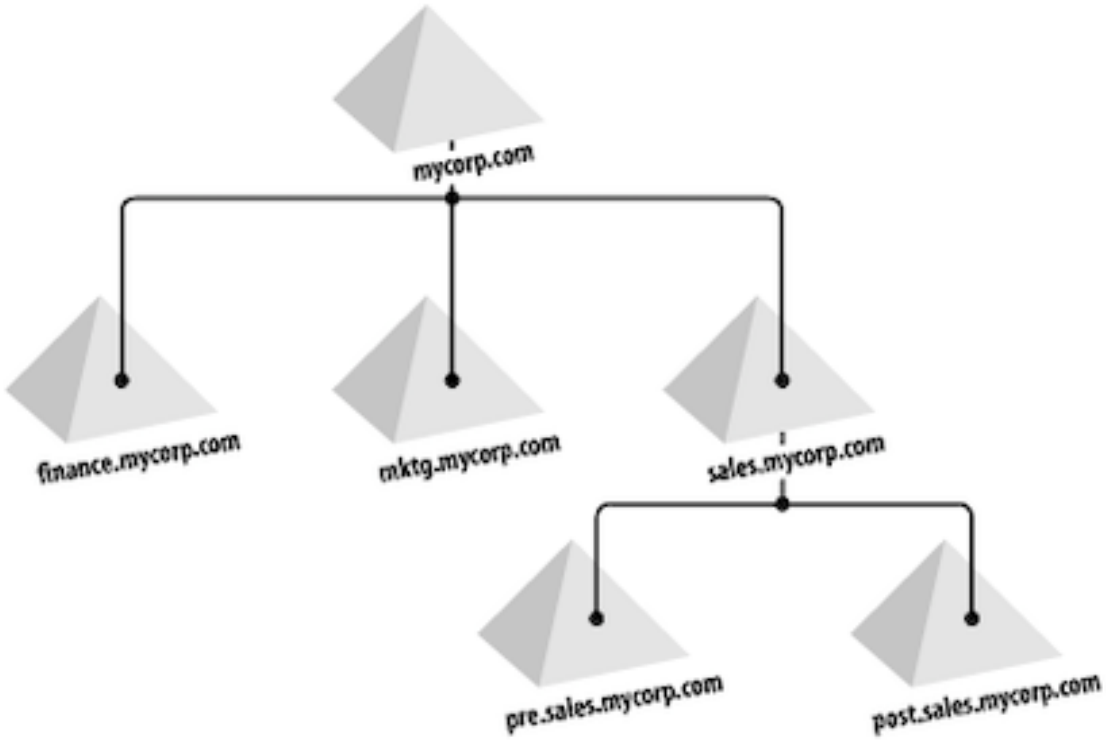

FIGURE 3. mycorp.com domain tree. (Allen & Lowe-Norris, 2003,11)

Active Directory Forest is the highest-level logical container (Figure 4). Forest can have one or more trees that contain domains. These domains trust each other, and that way forest is a security boundary of trust in company's Active Directory. (Microsoft documentation, What are Domains and Forests?, 2014).

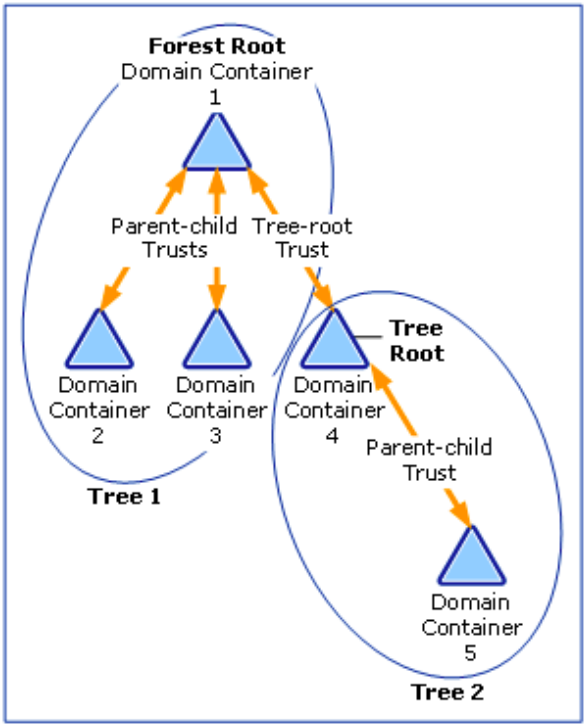

FIGURE 4. AD forest example (Microsoft documentation, What are Domains and Forests?, 2014).

This is a high-level overview of Active Directory. Active Directory is a wide and complex subject that has been used for years and would deserve a whole thesis work by itself. In this thesis I have only tried to give basic summary so that Active Directory integrations are easier to understand.

6.2 Active Directory integration

Active Directory is used in both Sandvik and DSI Underground. In the integration process there is a need to integrate identity and access management so that employees from DSI can be able to use Sandvik systems and services. This identity and access management is done in Active directory and for that reason it is a major aspect of IT security.

In Sandvik and DSI case, the first thing is again getting a security baseline from acquired company's Active Directory. There are third party solutions that can be used to check the security status of Active Directory. These third-party tools have an inbuilt set of rules that they test against Active Directory.

Some of the results that they will provide, are information about user counts, inactive user counts, domain admin accounts, possible vulnerabilities in domain controllers and existing trusts. These results should be thoroughly examined with the acquired company IT staff, and advice on fixing or mitigating them should be provided by the acquiring company if necessary. This process will again take time because changes to Active Directory should be considered carefully, and the actions are time consuming.

The acquired company should strive to cut down on the number of domain admins and inactive users, or at least find out the reason for these. If there are existing trusts between different domains, these should be severed and objects behind those trusts should be migrated to acquired company Active Directory. This migration should only be done if those objects need access to the acquirer company's resources.

When the findings in the acquired company's Active Directory have been fixed or mitigated, it is time to make decisions on, how will the integration of two Active Directories be done.

For this integration there are two choices. Start migrating users and computers from the acquired company Active Directory to the buying company AD or create a trust between those two Active Directories. The trust is in my opinion, faster and easier to create as both Active Directory forests will stay the same. It is also possible for the trust to be created first, and for the users and computers to still be migrated later.

Forest trusts help supporting access to objects and resources in multiple AD forests and are that way helpful for companies undergoing mergers. With forest trust, two different Active Directory forests are linked by two-way or one-way trust relationship (Figure 5). This forest trust will help administrators provide a seamless authentication and authorisation experience across forests. (Microsoft Documentation, How trust relationships work for resource forests in Azure Active Directory Domain Services, 2021)

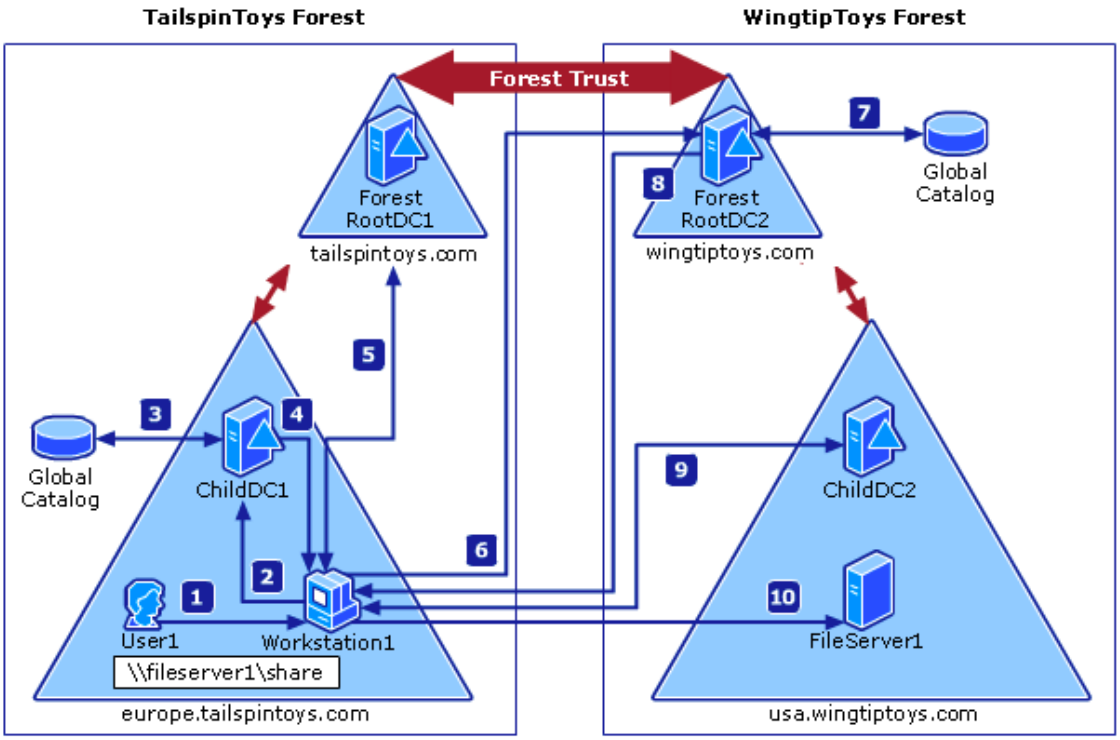

FIGURE 5. AD forest trust example (Microsoft Documentation, How trust relationships work for resource forests in Azure Active Directory Domain Services, 2021)

In my opinion, this forest trust is the way that active directory integrations should ne done. In this forest implementation the acquiring company creates a forest trust between its own root domain and the acquired company root domain. This should only be done, after the acquired company active directory has been examined and secured up to good standard. This will give a relatively easy way to integrate the two companies and enable collaboration and resource sharing.

This trust relationship in the two companies' active directories means that it is possible for the acquired company employees to get access to the acquiring company resources, but it does not mean that they will be granted the access right to do so. It provides possible access way but not by default the access right. Access rights are still up to the administrators to define and set up.

When the forest trust has been set up the administrators can start setting up different access right groups and rules. This is always done according to the principle of least privilege. According to this principle, the access rights should never be wider that is absolutely necessary.

7 ASSET MANAGEMENT

Asset management is big part of company governance. The basic premise is that assets need to be known before they can be secured and managed. This section goes through how asset management is present in acquisitions and integration process. With new acquisition there usually comes new assets that need to me documented and they need to be managed. The term assets include lots of different hardware and software elements, but this thesis will concentrate on the ones that are most important in the integration process.

7.1 Sandvik policy statement

In Sandvik Way are Sandvik IT Security policy. This IT Security policy has a statement regarding assets. It states that all IT hardware and IT software assets installed shall be assessed and documented. All IT assets connected must, regardless of ownership, be fully documented. (Sandvik IT Security Procedure, 2020)

This sets the overall framework that needs to be followed in asset management, and this is also what is required from an acquired company when integration starts. There is a need to document and assess all the assets in the acquired company and then start working out, that what solutions, if any, will stay in use and what will be replaced by Sandvik solutions. This is regarding the software assets, but hardware assets must also be charted, documented and assessed for mandatory IT security controls.

In mergers and acquisitions, after the acquired company employees have received their digital identities and user accounts, they can have access to acquiring company internal policies and procedures regarding asset management. From these documents they can learn what is required and expected of them at asset management. After this, these employees can take these requirements to their company and start gathering the necessary information on assets and implementing these procedures.

7.1.1 Configuration management database

Sandvik uses configuration management database in ServiceNow to document hardware assets and a central repository to document software assets. In Sandvik Way there is an IT Asset Procedure to guide asset management. The purpose of the procedure is that failing to keep track of IT assets exposes Sandvik to risks of legal, regulatory and contractual violations, as well as the business risks of failing to operate them properly. (Sandvik IT Asset Procedure, 2019)

Sandvik IT asset procedure lists mandatory asset information that needs to be documented. Asset categories in the scope of this procedure are IT asset, IT software asset, IT system asset, IT hardware asset, networked IT asset, server asset and software license.

This thesis will concentrate on, integrating server assets to the acquiring company IT infrastructure. IT asset procedure should list out all the mandatory information fields that need to be filled for assets to be compliant. This will probably also be required from the acquired company. For this to be as easy as possible, those key employees from the acquired company, should have been documented into the HR system to get employee IDs and Active Directory accounts to them. If this is not done at this stage, these employees are unknown in different company systems, and for this reason, they cannot be assigned to any roles regarding assets in configuration management database.

7.1.2 Mandatory information for server assets

In this chapter, this thesis goes through some industry best practices on asset management, and there are also some examples from Sandvik introduced. In ServiceNow’s configuration management database, company can decide how much and what information it wants to record.

First necessary information for servers will be the server’s name. It is always good practice to use some predefined naming convention, so the names will be uniform and possibly so that users can get some information about the server straight

from the name. For example, the name could include some information about the server location.

Second important information field could be the server owner. This is used in Sandvik and according to asset management procedure, this is a real physical person with contractual connection to Sandvik, that is accountable of the IT asset. This person needs to be in the HR system and needs Active Directory account to be eligible for the owner role in CMDB.

Configuration management database could have many additional information fields for the server. Some of these are very technical and some are related to employees by roles assigned to them. All these are up to every company to decide by themselves. When these are decided, it is best practices to document the needed information fields to IT asset procedure or some similar document.

For example, Sandvik records the environment that the server is used, this is the information whether the server is in test, development or productions environment. Servers' lifecycle status, which tells if the server is in use or possibly being decommissioned, and also information on who manages the server and how it is patched.

Most of the usual information recorded from servers are technical information that doesn't really have any dependencies. It is the roles and responsibilities area where the problems can arise. This comes again back to the fact, that employees need digital identities and user accounts to be able to assume any roles or responsibilities in the organisation. Information about who manages the server or what group is responsible of change management on the server are examples of these kind of dependencies.

For the newly acquired company, after servers have been registered to CMDB, new support and change groups need to be created inside configuration management database and these new employees added to those groups. Employees that are assigned to the support group, will be the ones that incident tickets get routed to. For this reason, they will also need ITIL access to CMDB.

8 APPLICATIONS

Modern enterprises can be using hundreds or even thousands of different applications daily. Managing these takes time and resources. When a new company is acquired, they are also using many applications and these applications might be completely different from what the acquiring organisation uses. Integration process needs time to make decisions on what application will be kept in use and to evaluate these applications.

8.1 Software that stays in use

The acquired company can have many different software applications in use that are not used in the acquiring company. The company may have been using these applications for years and built their business completely around them. Replacing all these applications with the ones used in the acquiring company may not be feasible or even something to be desired. This is why there needs to be some planning on what systems will continue to be used.

Decisions on what software will be kept in use, should be based, on what software will support the acquired company business best, and not what is used in the acquiring company. There is no value in replacing the acquired company software solutions if this hinders their business or growth. This might also undermine those value creation reasons for the whole acquisition.

There needs to be a thorough inventory of the software assets in use and discussion and planning on, what will be kept and what will be replaced. This requires a lot of knowledge, on how the acquired company is utilizing these solutions. There can be lot of business-critical software that cannot be easily replaced, or at least without lot of training and costs associated with it. There can also be some software assets that have licensing contracts running that cannot be ended straight away. On these solutions, there must be a decisions made, that if the software is replaced those contract costs still need to be handled.

8.1.1 Central Software repository

After there has been a thorough inventory and the software that will be kept in use has been identified, those software assets need to be documented. For example, Sandvik has a central software asset repository where this information is stored. Sandvik also has a central repository for storing software licensing information. When the acquired company, with the help of the integration team, has identified the software to be kept, they will document them into these central software repositories, and need to get all the required information fields filled.

When the application information is filled to this repository, there are some mandatory information, although less that with hardware assets. The application in repository needs to have unique ID, Owner of the application and software lifecycle status. Owner of the application will be, in Sandvik's case, the person at Sandvik, accountable for the costs and risks related to Sandvik's use of an IT asset. In Sandvik, this owner will for example be accountable on the costs of the applications and in the case of risks, they will have to make decisions on investments to mitigate these risks or accepting them. Software lifecycle status is the information that, is the application in use, still coming up to be used or being retired. Applications also need to be assessed for how business critical they are, and this assessment will tell about the security controls required from them.

8.1.2 Assessing software assets

Software assets that are to be kept in use will become part of acquiring company software portfolio. These applications will need to be assessed for their risk level. This assessment is done as a business impact analysis. In this analysis the goal is to understand what information is processed in the solution. What parts of acquiring company business is that information concerning. This is done by trying to understand what end to end business process the solution is supporting. For example, is it sales information or information relating to production. There is also a need to understand if there is any personal information stored or processed in the solution as this will have regulatory implications from GDPR.

Once the nature of information stored and processed in the solution is known it will be assessed from different viewpoints. This impact assessment is done jointly by IT Security and stakeholders from business side who are the ones using the solution. There is a thorough impact assessment where the business impact is analyzed, if the information confidentiality is compromised, integrity of the information is compromised, or the information is no longer available. All these aspects need to be assessed as they can have very different impacts on business.

From this business impact analysis comes the risk level for the solution. If assessment results show that, in a possible information compromise event the impact for business would be major, this sets higher security requirements. This risk level gives information on what IT security controls must be implemented for the solution. This business impact analysis is only assessing the impact on possible compromise of the solution and not the probability of it happening. The basic premise is that if the impact would be high, there is a need to reduce the probability of this occurring with set security controls.

There is also a need to assess how the solution is delivered. Is it running in the cloud or is it on premise. If it is a SaaS solution for example, the vendors security controls must be assessed. One possible tool for this assessment, is to have the vendor fill out CAIQ document (Example of questions in CAIQ, Appendix 1). This is a standard questionnaire provided by the Cloud Security Alliance.

There should always be a thorough assessment of the existing security controls, regardless of the delivery method. Assessed risk level of the solution should dictate the level of security controls required. This assessment is part of assessing the probability of the business impact being realized. If the initial business impact analysis shows that the business impact of compromise in the system would be major, there might be the need to add additional security controls to mitigate that risk.

9 DISCUSSION

This thesis work tried to chart the integration process starting from the pre-transaction phase of acquisitions. This is because the integration work starts in the pre-transactions phase as the information from due diligence process is needed for the integration process. Integration planning also starts when the acquisition targets IT infrastructure has been charted and evaluated. When the acquisition targets IT infrastructure has been mapped out, investigation of dependencies and any shortfalls in the IT security can start.

9.1 Acquisitions security posture

In the integration process it is crucial to get a complete picture of the acquisition targets IT infrastructure and security posture. Planning for any changes cannot start before the existing solutions are known. The acquired company's policies and procedure documents, if there are any, are a valuable source.

When complete access to the information is gained, IT solutions used in the acquisition target need to be thoroughly investigated. There is a need to examine, the network solutions in use and list all assets that the company has, this includes all hardware, software and licences. If the company has any joint ventures, how IT has been organized between them and if there are any existing connections or trusts, should be investigated. All existing contracts and agreements that the acquired company might have, need to be reviewed with a legal team. It is good practice to do interviews and site visits to truly confirm the information provided about the assets and IT infrastructure.

When there is a good understanding of what the acquired company's assets and infrastructure comprises of, possible changes can be planned. if there is a plan to make any changes, decisions also need to be made, about what existing solutions to keep and what to actually change.

9.2 Integration and dependencies

Once the acquired company IT assets and infrastructure has been investigated and mapped out, planning for the necessary changes starts. The underlying goal is to get the acquired company IT security posture up to a good standard, so that when any integrations and connections are implemented, any new risks aren't accidentally imported to the existing IT infrastructure.

In Sandvik there are policies and procedures that govern IT. If the acquired company does not have any policies or procedures of their own, there is no need to start producing them at this point. Many different integration streams can run parallel, during the integration process. Key employees from the acquired company need to be chosen, they have to get access to policies and procedures and access to start learning these procedures and that way start implementing the new way of working into the acquired company.

At the same time as implementing new policies and procedures to the acquired company, and if there is a good picture of the existing IT infrastructure and security posture it is good time to start making decisions on what technologies to keep and what to change. There might, for example, be a need to change anti-malware systems, implement vulnerability scanning on different levels, make changes to Active Directory, change networks layouts and configurations, change multitude of security configurations and rules and make impact and security assessment of the used solutions.

All this works toward the goal of getting the acquired company's IT security on a required level so that it is safe to start making connections. It is kind a two-step process and very intuitive one. First, the new IT realm should be secured up to company's standards, and then there can be connections and integration starts between existing and the new IT infrastructures.

It is in the connecting and integrating phase when the dependencies become a problem. Before integration, there is no need to concentrate on any dependencies, but they should be acknowledged from the beginning.

When the acquired company IT security posture is up to good standard and the time arrives to start making connections, then there needs to be a right sequence for integrating systems.

For example, many IT systems in Sandvik need a real person and this means a Sandvik employee to be recorded as responsible or accountable of any system. For this to be possible that person needs to be in Sandvik HR system in one way or the other. They need an employee id and username. Before this they are unknown to Sandvik systems.

Using Sandvik as an example, if there aren't any employees in the acquired company, that have Sandvik employee id and user account, they cannot be recorded to any necessary roles in Sandvik systems. This means that the acquired company's hardware assets can't be registered to CMDB, applications can't be registered to software repository and employees don't get access to Sandvik Way and any collaboration tools.

9.3 Critical evaluation

This thesis work was done when the DSI integration was still ongoing. These integration processes are very complex and long projects, and they are unique on each case. There were still lot of unknown information, on how the DSI underground integration would be implemented, and because of this, it could not be made available in this thesis.

This thesis had to make lot of information generic, that would apply to many future integration projects because the DSI integration was not finished at the time of writing this thesis. This meant, that not all the integration decisions were clear at the time. The DSI underground integration process will run at least one more year after this thesis was finished. Still, observations made in this thesis, will aid in planning future integration projects.

REFERENCES

Allen, R. Lowe-Norris, A. 2003. Active Directory. 2nd edition. Sebastobol: O'Reilly Media.

Microsoft documentation. 11.01.2022. Active Directory Domain Services Overview. Read on 09.04.2022. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Microsoft Documentation. 29.12.2021. How trust relationships work for resource forests in Azure Active Directory Domain Services. Read on 09.04.2022. https://docs.microsoft.com/en-us/azure/active-directory-domain-services/concepts-forest-trust

Microsoft documentation. 19.11.2014. What are Domains and Forests?. Read on 09.04.2022. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759073(v=ws.10)

Sandvik Acquisitions and Divestments Policy. 2021

Sandvik Identity and Access Management Procedure, 2018

Sandvik IT Asset Procedure, 2019

Sandvik IT Policy, 2020

Sandvik IT Security Policy, 2020

Sandvik IT Security Procedure, 2020

Sandvik M&A Procedure. 2021

Sandvik M&A Procedure Part 1 – Acquisitions, 2021

Sandvik M&A Procedure Part 3 – The Sandvik Way Implementation, 2021

Sandvik Powerpoint. Integration options in acquisitions. 2019

Sandvik Way description, Sandvik intranet. 2022

APPENDICES

APPENDIX 1. Example of questions in Consensus Assessments Initiative Questionnaire (CAIQ). www.cloudsecurityalliance.org. Modified.

Example of questions in CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE

Control Domain	Consensus Assessment Questions
Application & Interface Security *Application Security*	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?
	Do you use an automated source code analysis tool to detect security defects in code prior to production?
	Do you use manual source-code analysis to detect security defects in code prior to production?
Audit Assurance & Compliance *Independent Audits*	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?
	Do you conduct network penetration tests of your cloud service infrastructure at least annually?
Business Continuity Management & Operational Resilience *Business Continuity Planning*	Does your organization have a plan or framework for business continuity management or disaster recovery management?
	Do you have more than one provider for each service you depend on?
	Do you provide a disaster recovery capability?
Business Continuity Management & Operational Resilience *Equipment Location*	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?
Business Continuity Management & Operational Resilience *Retention Policy*	Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?
	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?
	Do you test your backup or redundancy mechanisms at least annually?
Change Control & Configuration Management *Unauthorized Software Installations*	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?

	Can you ensure that data does not migrate beyond a defined geographical residency?

Data Security & Information Lifecycle Management *E-commerce Transactions*	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?
	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?
Data Security & Information Lifecycle Management *Nonproduction Data*	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?
Datacenter Security *Asset Management*	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?
	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?
Datacenter Security *Controlled Access Points*	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?
Datacenter Security *Offsite Authorization*	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?
Governance and Risk Management *Baseline Requirements*	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?
	Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?
Governance and Risk Management *Policy*	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?
	Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?
	Do you disclose which controls, standards, certifications, and/or regulations you comply with?

Identity & Access Management *Audit Tools Access*	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?
	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?
Identity & Access Management *User Access Policy*	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?
	Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements?
	Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege?
	Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?
Identity & Access Management *Policies and Procedures*	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?
	Do you manage and store the user identity of all personnel who have network access, including their level of access?
Identity & Access Management *Source Code Access Restriction*	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?
	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?
Identity & Access Management *User Access Restriction / Authorization*	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?
Identity & Access Management *User Access Reviews*	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?
	Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?

Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?
	Is physical and logical user access to audit logs restricted to authorized personnel?
	Are audit logs centrally stored and retained?
	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?
Infrastructure & Virtualization Security *OS Hardening and Base Controls*	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?
Infrastructure & Virtualization Security *Segmentation*	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?
	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?
	Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations?
	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?
	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?
Infrastructure & Virtualization Security *Network Architecture*	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?
	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?

Security Incident Management, E-Discovery, & Cloud Forensics *Incident Management*	Do you have a documented security incident response plan?
	Do you integrate customized tenant requirements into your security incident response plans?
	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?
	Have you tested your security incident response plans in the last year?
Security Incident Management, E-Discovery, & Cloud	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?

Forensics *Incident Response Legal Preparation*	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?
	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?
Supply Chain Management, Transparency, and Accountability *Incident Reporting*	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?
Supply Chain Management, Transparency, and Accountability *Third Party Agreements*	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?
	Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?
	Does legal counsel review all third-party agreements?
	Do third-party agreements include provision for the security and protection of information and assets?
	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?
	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?
	Can you provide the physical location/geography of storage of a tenant's data upon request?
	Can you provide the physical location/geography of storage of a tenant's data in advance?
	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?
	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?
	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?
	Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?

Threat and Vulnerability Management *Antivirus / Malicious Software*	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?
	Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?
Threat and Vulnerability Management *Vulnerability / Patch Management*	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?
	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?
	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?
	Will you make the results of vulnerability scans available to tenants at their request?
	Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?
	Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?