Robin Metsäranta

Creating a Plan for Identity Management During System Changes.

Metropolia University of Applied Sciences

Bachelor of Engineering

Industrial Management

Bachelor's Thesis

28 January 2021

Author Title Number of Pages Date	Robin Metsäranta Creating a Plan for Identity Management During System Changes. 45 pages 28 January 2021
Degree	Bachelor of Engineering
Degree Programme	Industrial Management
Professional Major	ICT
Instructors	Anna Sperryn, Senior Lecturer Jasmin Sauren, IAM Lead

The purpose of this thesis was to provide a starting point in the form of a plan for the customer company, which addresses the identity management of the external workforce, during large system changes within the company. In the current state the future management of the external workforce is still unclear resulting in the need for exploring the process during the transition and target states of the system changes.

Information used for creating the plan was obtained by discussing with people inside of the company to gain various different viewpoints about the identity management of externals. The thesis also utilized existing company documents and relevant literature.

The final outcome of the thesis consists of a conceptual data model for vendor access management in the target state, application landscape models for the current, transition and target states. The thesis also provides views on the business architecture, process ownership and definitions within the vendor access management process.

Keywords

Tekijä Otsikko Sivumäärä Aika	Robin Metsäranta Suunnitelman luonti identiteetinhallinnalle järjestelmämuutosten lähestyessä. 45 sivua 28.1.2021
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	Tuotantotalous
Ammatillinen pääaine	ICT
Ohjaajat	Anna Sperryn, Lehtori Jasmin Sauren, IAM Lead

Tämän opinnäytetyön tavoitteena on tarjota lähtökohta asiakasyritykselle, joka ottaa kantaa ulkopuolisen työvoiman hallintaan isojen järjestelmämuutosten lähestyessä. Nykyisessä tilassa ulkopuolisen työvoiman tuleva hallinta on vielä epäselvä, mikä luo tarpeen katsaukselle identiteetinhallinan prosesseihin järjestelmämuutosten eri vaiheissa.

Tietosisältö suunnitelman luontiin hankittiin yrityksen sisäisten keskustelujen kautta. Tiedon keräämisen tavoitteena oli saada useita eri näkemyksiä ulkopuolisten identiteettien hallinnasta yrityksen sisältä. Opinnäytetyössä myös hyödynnetään olemassa olevia yrityksen dokumentteja ja relevanttia kirjallisuutta.

Opinnäytetyön lopullisiin tuloksiin kuuluvat käsitteellinen datamalli ulkopuolisen työvoiman hallinnasta tavoitetilassa ja applikaatio maisemamallit nyky-, transitio- ja tavoitetiloissa. Opinnäytetyö myös käsittelee liiketoiminta-arkkitehtuuria, prosessin omistajuutta sekä määritelmiä ulkopuolisten identiteetinhallinnan prosessin sisällä.

Avainsanat	

Contents

List of Abbreviations

IdM Identity management. The organizational framework for ensuring that individuals have the appropriate access to technology resources.

HCM Human capital management. A set of practices for people resources management.

CSA Current state analysis. An evaluation of a business’s current processes.

ERP Enterprise resource planning. Integrated management of main business processes.

HRMS Human resources management. system A system for managing human resources.

PACS Physical access control system. A system for managing a business’s physical accesses.

ACMS Active card management system. A system for managing a business’s keycards.

1 Introduction

Identity and access management is a term for frameworks and technologies inside a company, which makes sure that people in the organization have the necessary access privileges for their role within the company. The identity management of a company is often managed with the use of an IdM system.

In the modern day, it is key for organizations to ensure that the right people have their own set of access rights within the company. It is also extremely important to make sure that people's identities within the organization are protected and that the information which the identities can interact with are carefully defined and appropriately limited.

1.1 Business context

The customer company Vaisala Oyj is a global leader in weather, environmental and industrial measurement. Vaisala develops and manufactures products to customers in over 150 countries. Vaisala has offices across the world including in Finland, Europe, America and Asia.

This thesis focuses on the identity management of Vaisala's external workforce within the changing landscape of Vaisala's internal systems.

1.2 Business challenge, objective & outcome

With a new human capital management system on the horizon, the position and management of the identities of the eternal workforce needs to be re-designed. In the current state, there are some issues in the management of these types of identities that could be improved.

Creating a plan for managing the identities of the external workforce is necessary for the customer company before the actual changes in the systems are completely carried out.

The objective of this thesis is to create a plan, which takes into account three different stages of the identity management of the external workforce. First, the plan will consider what changes need to be done to enter the transitional phase when the new HCM system is implemented. Secondly the plan will take into account the transition into the permanent stage of the identity management when the changes have been completely implemented. Finally, the plan examines the maintenance of the identities of the external workforce after the changes by exploring the needs of the process and the changes in roles that the transition will create.

The outcome of the thesis is a comprehensive plan taking into account the needed various stages of identity management to prepare for future system changes.

1.3 Thesis outline

This thesis begins with analyzing the current state of the external workforce from the perspective of identity management. The data used in this thesis was procured from preexisting data from customer company and from interviews. With the help of the findings in the data and literature a plan for managing the migration and maintenance of the external workforce was created.

The thesis begins with an introduction to the key themes and objectives of the study, afterwards in section two, the study introduces the different methods and materials used in the study with the addition of a plan and a schedule for producing the study. Section three focused on the current state analysis of the customer company, looking at the strengths and weaknesses of the current state of the external workforce's identity management. Section four gives on overview of the relevant literature in the field of identity management to aid this project. In section five a first draft of the plan was built and in section six it was reviewed, evaluated and modified to match the requirements of the customer company. Finally, section seven concluded the study with a summary and review and reflections on the subjects covered in the thesis.

2 Methods and material

This section introduces the different methods and materials utilized in this thesis ranging from the research approach and design to data collection, project plan and schedule. To illustrate the time management and scheduling of this project and the logical progression of gathering information and formulating the plan, relevant graphical illustrations have been created in addition to the text.

2.1 Research approach

The methods for approaching the business challenge can be divided into four different key categories. Firstly, the thesis strived to find relevant literature and about the subject and to refine the findings to their key ideas in order to further advance and aid in the progression of the plan. The thesis explored literature about identity management from a theoretical standpoint and also look into real-life applications and case-studies. Secondly, the thesis explores information found by discussing with key people in the customer company. Thirdly, the findings were refined and developed by working closely with advisors from both the customer company and university. Finally, the combination of research and data was used in the plan building and validation stage to produce the final result.

2.2 Research design

The following figure displays the research design, data collection points, outcomes of this thesis and the methods used in the process to reach those outcomes.

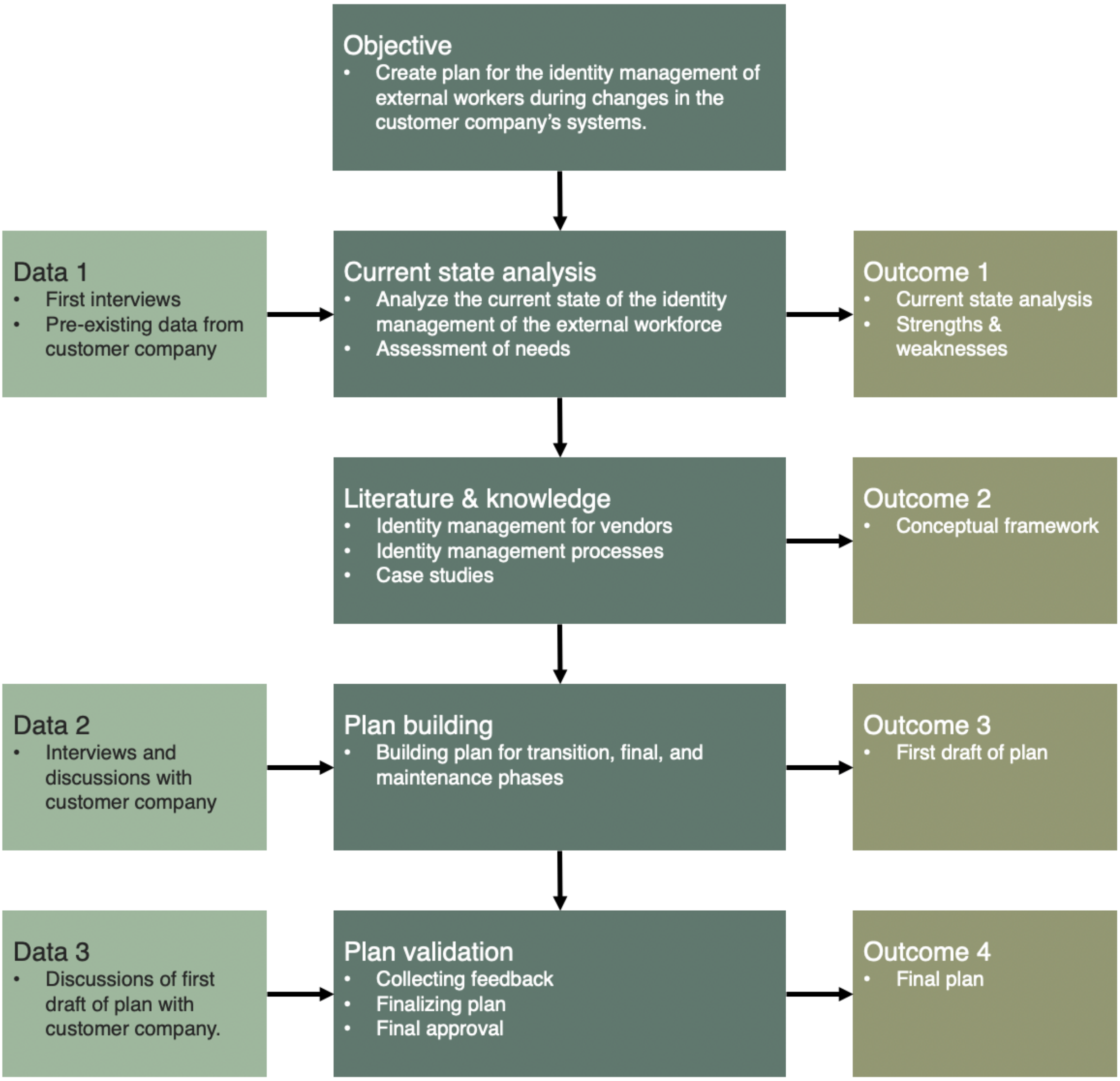

Objective
• Create plan for the identity management of external workers during changes in the customer company's systems.
Data 1
• First interviews
• Pre-existing data from customer company
Current state analysis
• Analyze the current state of the identity management of the external workforce
• Assessment of needs
Outcome 1
• Current state analysis
• Strengths & weaknesses
Literature & knowledge
• Identity management for vendors
• Identity management processes
• Case studies
Outcome 2
• Conceptual framework
Data 2
• Interviews and discussions with customer company
Plan building
• Building plan for transition, final, and maintenance phases
Outcome 3
• First draft of plan
Data 3
• Discussions of first draft of plan with customer company.
Plan validation
• Collecting feedback
• Finalizing plan
• Final approval
Outcome 4
• Final plan

Figure 1. Research design

The left side of figure 1 shows the various data collection points during the project. First, we have the initial interviews and pre-existing data in Data 1. In data 2 we have the interviews and discussions used to progress the plan building process. In data 3 we gave the discussions considering the first draft of the plan.

The middle of the figure shows the different stages of the project, starting from defining the objective. After the objective, the figure displays the current state analysis of the identity management of the external workforce. There is also the literature and knowledge part of the research design which encompasses the relevant literature and pre-existing knowledge used to progress the thesis. After the literature analysis, the figure shows the plan building stage and finally the plan validation stage.

The right side of the figure displays the different outcomes resulting from the different stages of the project beginning from the outcomes of the current state analysis stage. The second outcome is the conceptual framework of the study, which is a result of the literature analysis. The third outcome is the first draft of the plan, which is a result the plan building stage. The final outcome of the research is the is the final plan which is the result of the validation stage.

2.3 Data collection and analysis

The data collection for this thesis is divided in three parts. The first data table presents the data used for building the CSA. The second table shows the data for building the first draft of the plan. And finally, the data for refining and validating to arrive at the final version of the plan is displayed in the third table.

Table 1. First stage of data collection

	Participants / role	**Data type**	**Topic, description**	**Date**	**Key points**
	Data 1, for the Current state analysis				
1	IAM Lead Enterprise architect Business Solution Owner, Projects & HR	Meeting notes	Explanation of current IdM process	2020-09-29	Conceptual model should be utilized in CSA. Role of PACS in IdM
2	HR personnel IAM Lead	Meeting notes	Differentiating between Service workers and other external workers	2020-10-02	Differences between groups are

					challenging to establish. Conclusion was not reached
3	IAM Lead Facilities & Office Services Team Leader	Meeting notes	IdM process of Service contractors in Finland	2020-10-14	Scattered maintenance. Role of ACMS and PACS. Service worker process nonexistent,
4	IAM Lead Manager, IT Service Delivery	Meeting notes	CSA validation	2020-10-21	Strengths and weaknesses need to be revamped. Wording changes. Addition of process descriptions to CSA.
5		IdM process presentation	IDM processes_v2.0.pdf	2020-09-28	Descriptions of IdM processes
6		IdM definitions & principals presentation	Identity Management - Definitions Principals_v5.7.pdf	2020-09-28	Definitions. Principals, weaknesses in current state.
7		Vaisala IdM architecture presentation	Vaisala IDM architecture.pptx	2020-10-23	IdM architecture, system landscape and relationships.
8		Presentation on IdM workflows, user stories & lifecycles.	Vaisala IDM Functional design.pdf	2020-09-28	IdM workflows, user stories & lifecycles.

Data 1 presents first-round data and lists discussions conducted in the beginning of the project which were used in constructing the current state analysis. The discussions were held with employees in various different positions within the IT, HR and facilities departments.

Table 2. Second stage of data collection

	Participants / role	Data type	Topic, description	Date	Key points
	Data 2, for plan building				
1		IdM definitions & principals presentation	Identity Management - Definitions Principals_v5.7.pdf		Application architecture
2		Vaisala IdM architecture presentation	Vaisala IDM architecture.pptx		Application relationships
3	IAM Lead CIO	Meeting notes	Process ownership reasons	2020-11-19	Vendor access management process ownership
4		Solution guide.pdf	SG_Vendor_Access_Management.pdf	2020	Solution capabilities
5		Internal identity conceptual model	Conceptual data model for internal identities	2019-01-04	Conceptual data model for internal identities

Data 2 lists the discussions and documents used in building the initial draft of the plan. The data in the second table consists of pre-existing documents describing the current process, the capabilities of the IdM system and a discussion considering the ownership of the vendor access management process.

Table 3. Third stage of data collection

	Participants / role	Data type	Topic, description	Date	Key points
	Data 3, for plan validation				
1	IAM Lead	Meeting notes	Plan validation	2020-12-02	Application landscape and conceptual data model refining. Technology and security architecture.
2	IAM Lead	Meeting notes	Plan validation	2020-12-16	Terminology changes. Process ownership validation. Conceptual data model refining.
3	IAM Lead	Meeting notes	Plan validation	2020-01-19	Process ownership validation

Data 3 lists the discussions utilized in finalizing and improving the plan. The discussions were held with the thesis advisor to ensure the accuracy and validity of the plan.

2.4 Project plan and schedule

The project followed the GATE-system which divides the project into seven different sections. The progression of the project was also paced by the availability of the people necessary for conducting the CSA, plan building and validation stages. The following figure shows the different parts of the project and how they were scheduled between September 2020 and January 2021.

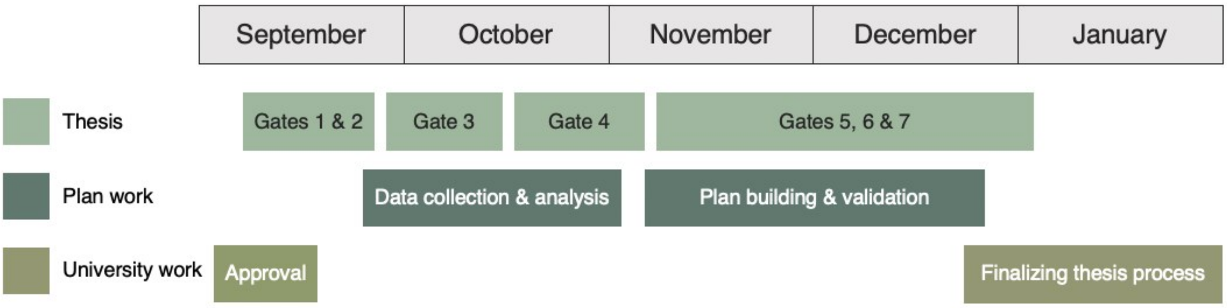


Figure 2. Project schedule

As can be seen in the schedule, the plan was divided into three different sections of work. First, the schedule shows the amount of work spent writing the thesis divided into different gates, which signify the parts of the written thesis. There is also the “Plan work” section, which shows the time spent on external work required for writing the thesis, including the data collection and analysis stages and the essential work required for building the plan and validating it. The third section “University work” displays the stages of the project where consulting the school was necessary for progressing the project. The final thesis was finished already after gate 7 at the beginning of January but the thesis process was not entirely complete until the university approved it in February.

3 Current state analysis

This section discusses the current state of vendor access management and identity management of the external workforce in Vaisala Oyj. This chapter first looks at the reasons for conducting the CSA and the uses for the outcomes of the analysis. After exploring the reasons for conducting the CSA, the chapter focuses on laying out relevant information about the current state of identity management considering the objectives of the study. Finally, the chapter closes with a concise strengths and weaknesses -analysis of the current state.

3.1 The Purpose for conducting the current state analysis

The purpose of the current state analysis was to gain information on the different aspects of identity management which need to be taken into account for formulating a useful plan for the future. Another of the purposes for the analysis was to find the weaknesses and strengths of the current state and how the different weaknesses can be improved by following the final plan.

By having a clear view of the current state, the steps for creating a successful plan became more apparent by attaining a deeper understanding of what needs to be done based on the current state.

This CSA is based on the initial meetings and discussions with the key people from the perspective of identity management inside Vaisala and pre-existing data and analyses from Vaisala. The thesis strived to create an honest and accurate description in the CSA to have a focused starting point in the plan building stage.

3.2 The current state analysis

Vaisala Oyj is a large company that develops, sells, and manufactures products thus having a large variety of employees with different roles, is expected. Some of these identities are considered external workers, they work for the company, but are not on its payroll. These external workers include for example, cleaning staff, parts of the manufacturing staff and IT consultants, in the current state the lines between the different types of external workers were defined.

In the current state, the IdM process for birthright accesses of the new external workforce starts when a manager or approver fills a from within the intranet and office services create an assignment in the HR system. The identity is automatically registered in the IdM system and its birthright accesses are automatically provisioned.

The following figure shows the current state of the application landscape surrounding the identity management of the external workforce.

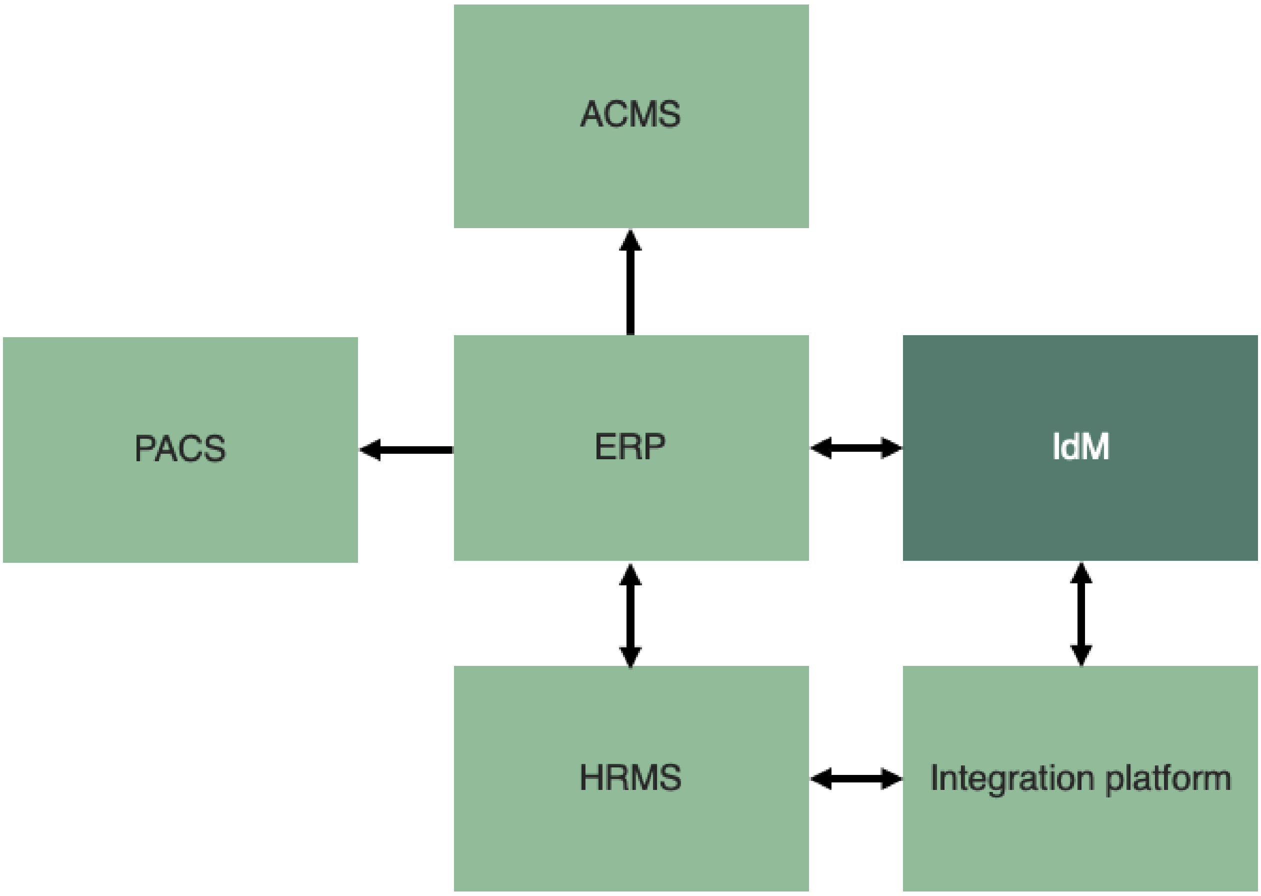


Figure 3. Application landscape in regard to IdM

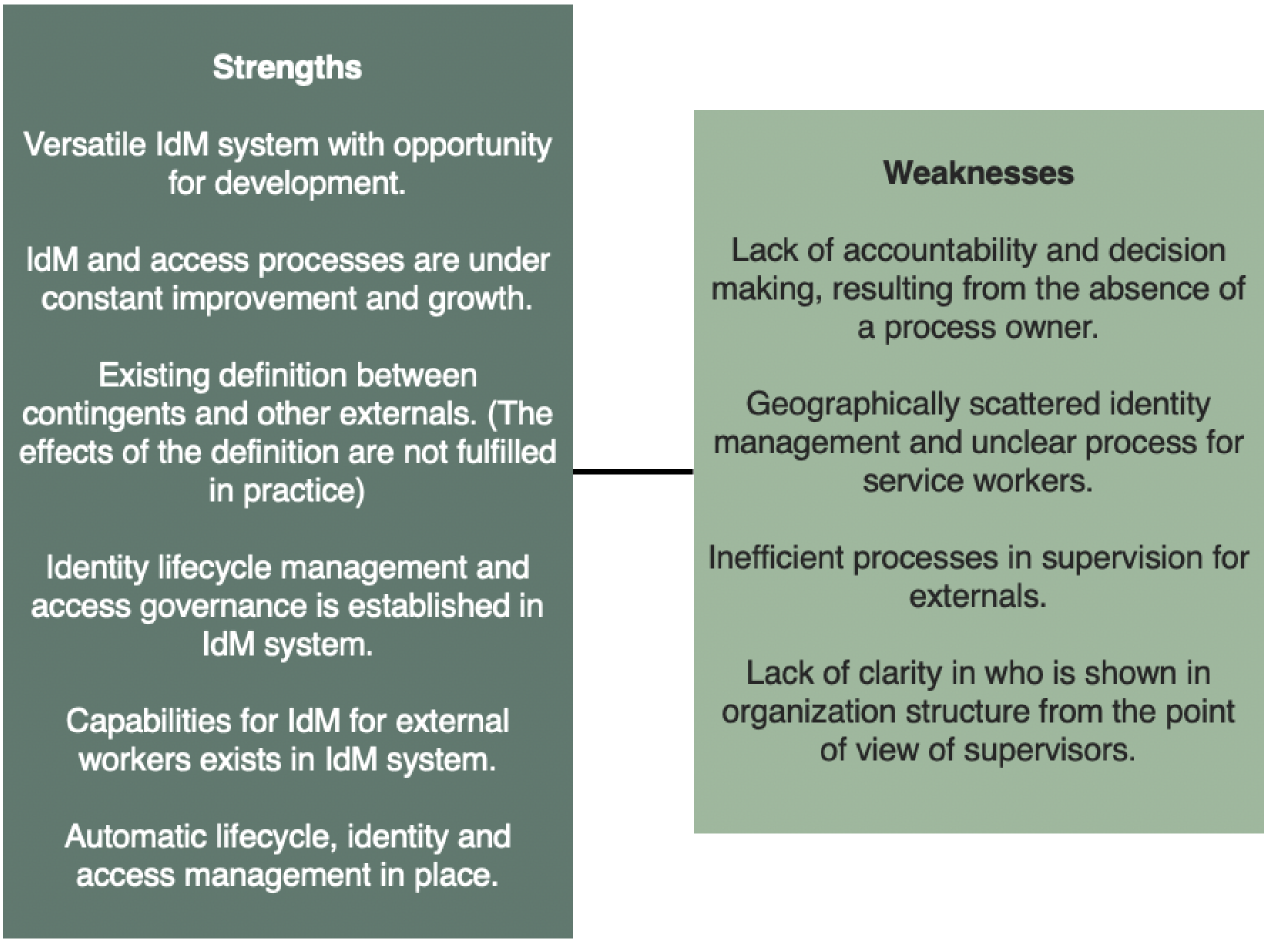
As seen in figure 3, Vaisala, in the current state has a designated IdM system, which manages the identities and accesses of all employees in Vaisala. Vaisala also has a HR management system which manages the HR data of most of the external workforce and employees. An integration platform is used for HR import, in the case of identity management, all communication between the IdM and HRMS is one by using the integration platform, the same is true for the ERP. The active card management system and the physical access control system are systems which handle the physical accesses and keycards of employees and the external workforce.

The key issues in the current state of vendor access management cause invisibility, lack of control and inefficiency in the identity management of service contractors. The vendor management concept does not have an owner, which results in a lack of direction and accountability in regard to decision making and future direction. The identity management of externals is scattered, the identities are managed by different teams and people dependent on the location of the worker and there are inconsistencies in who should be visible in the Vaisala organization structure. At the current state the process of bringing new externals to Vaisala is slightly inefficient and creates bureaucracy as only Vaisala employees in supervisory positions can act as an external worker’s contact person.

At the current state, the system landscape of Vaisala is under substantial changes. A new human capital management system is set to replace the existing HRMS, which affects the identity management of externals significantly. The state of the external workforce within these changes in the systems is still yet to be decided on. The IdM landscape is also under constant change and evolution due to the new functionalities and updates being added to the identity management system. As of now there is no owner for the external identity management process which causes issues in defining the attributes of external workers, and clarity in the application landscape considering the external workers.

Whenever there are new applications or integrations in the customer company it’s required to produce a VAM study (Vaisala Architecture Management Study). This study consists of various investigations in different aspects of architecture relating to the change with the objective of answering architectural questions related to GIT and enterprise architecture domains. With the VAM study being a necessary part of the types of changes this thesis considers, It’s included in the final plan.

The following figure displays the current strengths and weaknesses in the vendor access management process.



Strengths

Versatile IdM system with opportunity for development.

IdM and access processes are under constant improvement and growth.

Existing definition between contingents and other externals. (The effects of the definition are not fulfilled in practice)

Identity lifecycle management and access governance is established in IdM system.

Capabilities for IdM for external workers exists in IdM system.

Automatic lifecycle, identity and access management in place.

Weaknesses

Lack of accountability and decision making, resulting from the absence of a process owner.

Geographically scattered identity management and unclear process for service workers.

Inefficient processes in supervision for externals.

Lack of clarity in who is shown in organization structure from the point of view of supervisors.

Figure 4. Current state strengths and weaknesses

In the figure above there is a short list of weaknesses and strengths. Most of the strengths displayed are linked to existing systems and projects with potential for more development and improvements, whereas most of the weaknesses have to do with smaller process and definition-related issues. The weaknesses and strengths are kept in mind when moving forward with the project especially in the plan building stage.

3.3 Current state analysis conclusions

This current state analysis is the result of gathering information about the identity management of the external workforce from reviewing discussions with different stakeholders within the case company and collecting information from pre-existing analysis and materials from the case company. The purpose of the analysis was to create a clear view of the current state to enable a more straightforward plan building stage.

Overall the identity management is in a good position with most of the weaknesses being smaller and improvable. The constant improvement and growth in addition to the established automatized processes are vital strengths of the identity management process. Also, the capabilities of the existing IdM system look promising in terms of providing solutions to some of the weaknesses in the process.

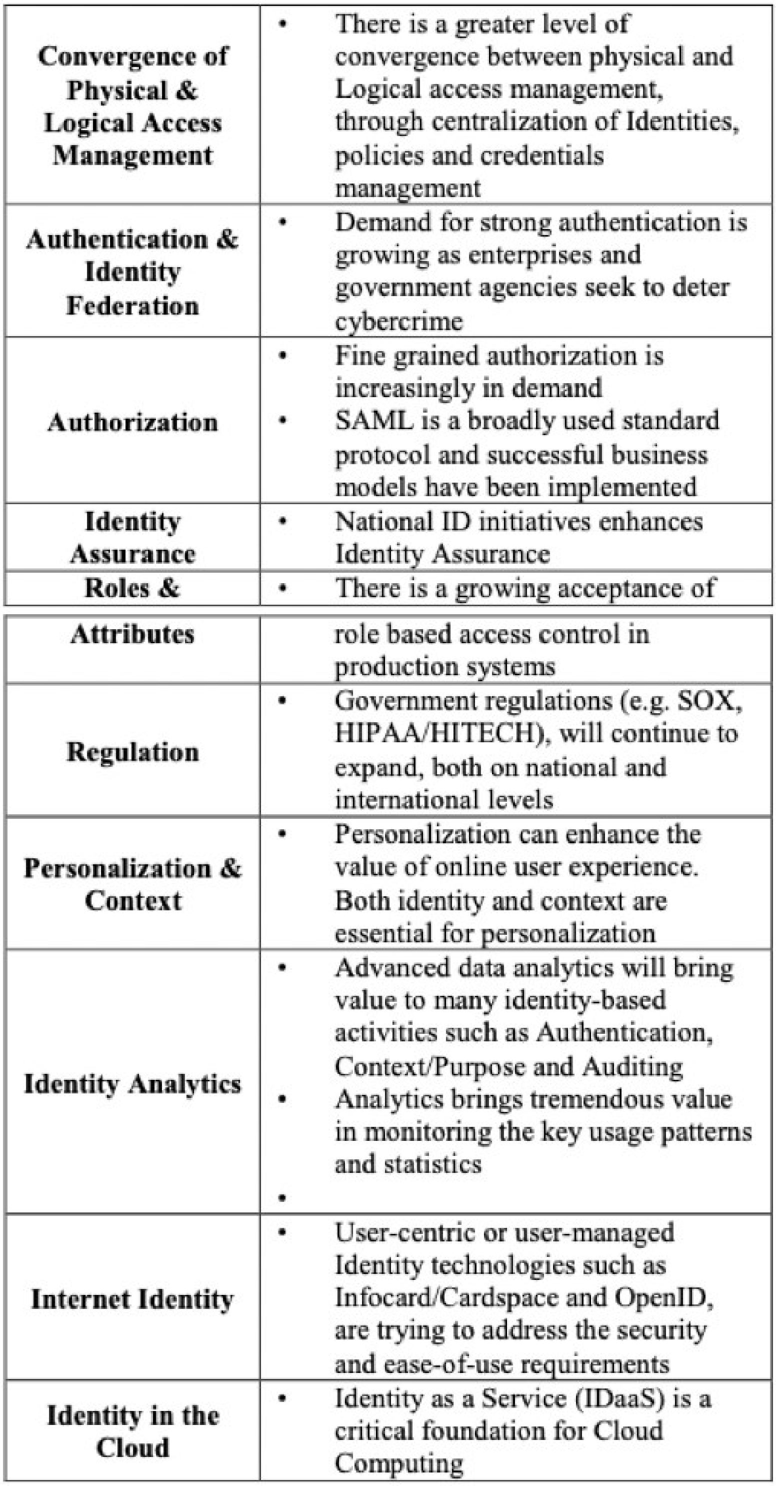
While this CSA focuses on many different aspects of identity management, it is important to keep in mind that the focus of the thesis was to create a plan amidst a changing software landscape and not necessarily attempt to tackle every weakness in the process. Rather, the weaknesses were points of interest which should be kept in mind when building the plan to make sure that the plan is a viable and functional transition from the current state to the target state.

4 Literature review

This section discusses the necessary literature for building a successful plan based on the factors shown in the CSA and the objective of the project. The first section takes a look at the basics and definitions of identity management to provide a clear understanding for the base of the plan. The second part specifically takes a look at vendor access management, to bring forth a form of IdM which is more closely related to the objective of the thesis. The third part discusses access management from the perspective of ITIL. The fourth section of the literature review considers the various purposes of process ownership in an IT context. The fifth section looks at the usage of conceptual data modeling with the objective of enabling the project team to create a viable model for the plan. Finally, this chapter summarizes the various literature that the thesis has included and explores the logical progression of the knowledge in the form of a conceptual framework diagram.

4.1 Identity management

Identity management is a unique and vital part of an organization which affects the organizations activities in many different aspects. The existence, or lack of control over a company's identities can have widespread influence over the success and development of a company's business. In order for a company to be able to successfully harness the potential of identity, it's necessary for the company to first have a sufficient grasp on trust and privacy. (Windley, 2008, p. 3-14) There are various different reasons for implementing identity and access management solutions such as security, business agility, cost containment, operational efficiency, IT risk management and regulatory compliance. (Al-Khouri, 2011) The following figure displays the various modern IAM trends.



Convergence of Physical & Logical Access Management	• There is a greater level of convergence between physical and Logical access management, through centralization of Identities, policies and credentials management
Authentication & Identity Federation	• Demand for strong authentication is growing as enterprises and government agencies seek to deter cybercrime
Authorization	• Fine grained authorization is increasingly in demand • SAML is a broadly used standard protocol and successful business models have been implemented
Identity Assurance	• National ID initiatives enhances Identity Assurance
Roles & Attributes	• There is a growing acceptance of role based access control in production systems
Regulation	• Government regulations (e.g. SOX, HIPAA/HITECH), will continue to expand, both on national and international levels
Personalization & Context	• Personalization can enhance the value of online user experience. Both identity and context are essential for personalization
Identity Analytics	• Advanced data analytics will bring value to many identity-based activities such as Authentication, Context/Purpose and Auditing • Analytics brings tremendous value in monitoring the key usage patterns and statistics •
Internet Identity	• User-centric or user-managed Identity technologies such as Infocard/Cardspace and OpenID, are trying to address the security and ease-of-use requirements
Identity in the Cloud	• Identity as a Service (IDaaS) is a critical foundation for Cloud Computing

Figure 5. IAM trends (Al-Khouri, 2011)

As can be seen in the figure above, there are many reasons and benefits for focusing on identity management in an organization. Implementing an IAM system however, does not automatically result in added value, if the system's position within the overall landscape is not carefully planned out. It's key that the IAM system can easily communicate and integrate with the organizations pre-existing systems in terms of lifecycle management and access provisioning. (Al-Khouri, 2011)

Application of IAM technologies may also pose challenges and risks, especially in terms of changes in workforce and operations in the implementation stage. Access from external sources, for example partners, may expose an IAM system to security risks in terms of access to sensitive internal information. (Al-Khouri, 2011)

An identity infrastructure has three key components which need to be taken into account when building an organizations identity management: process architecture, data architecture and technical reference architecture. The process architecture represents the methods and tasks of conducting identity management built with the purpose of answering the organizations identity management needs. The data architecture represents how and where the company's identity data is stored and maintained in order to avoid possible security issues and mistakes. The technical reference architecture answers the question: How should the company communicate with its different parts in terms of using and processing identity data. (Windley, 2008 p. 6-7)

An identity, at its core, determines two key features of a user, who are they and what are their relationships amongst other users and systems. An identity contains data which uniquely identifies a user and data which determines the user's position amidst other users and things, in the form of attributes, preferences and traits. (Windley, 2008, p. 3-14)

A key component of a digital identity is its lifecycle, an identities lifecycle displays the different stages of an identity, enabling a more holistic view and processing of the identities. The lifecycle of an identity begins in the stage of provisioning, where an IT system creates an identity and populates it with the necessary attributes. Propagation can be another stage of an identities lifecycle, where it's necessary for an identity to be propagated to other systems than the one it was created in. Using is another phase in the identities lifecycle, where the identity is currently in use of various systems. Maintenance of an identity is important when, for example, changes occur in the identity's attributes, which requires actions to keep everything working as intended. Deprovisioning is the stage of the end of an identity's lifecycle, which purpose is detaching the identity from the system to avoid possible security risks and confusion. (Windley, 2008, p. 3-14)

4.2 Vendor access management

The use of contractors and vendors is very common in modern organizations, a company might, for example hire IT consultants or cleaning staff from an external company. As these external non-employees often require access to for example software or network drives, it's key to decrease the possibility of non-employee risks by making sure that the vendor access management process accurately answers the needs created by the use of external workers. Without a specific process to manage external workers, managing their accesses and identity lifecycles can be challenging as they often differ from accesses and lifecycles of employees. (Saviynt, 2020)

The aforementioned non-employee risks can be reduced with a sponsor-based approach, where an internal sponsor manages the external workers account through its lifecycle and is able to have full visibility into the account's accesses. It's important for an organization to have practices set in place for external workers to ensure compliance and appropriate usage of accesses. (Saviynt, 2020)

4.3 ITIL

ITIL is the leading method for IT Service Management, going through multiple iterations with ITIL 4 being the latest. Services are one of the main methods companies create value and with IT being a key part of a modern company's operations and value, managing IT services successfully is crucial. It is important for a company and its individuals to have a grasp on the key components of ITIL to utilize its frameworks in an effective way. (Axelos, 2019, p. 13-15)

The core elements of the ITIL framework are the ITIL service value system and the four dimensions model. The service value system shows how the different parts and operations of an organization work together to create value. (Axelos, 2019, p. 13-15)

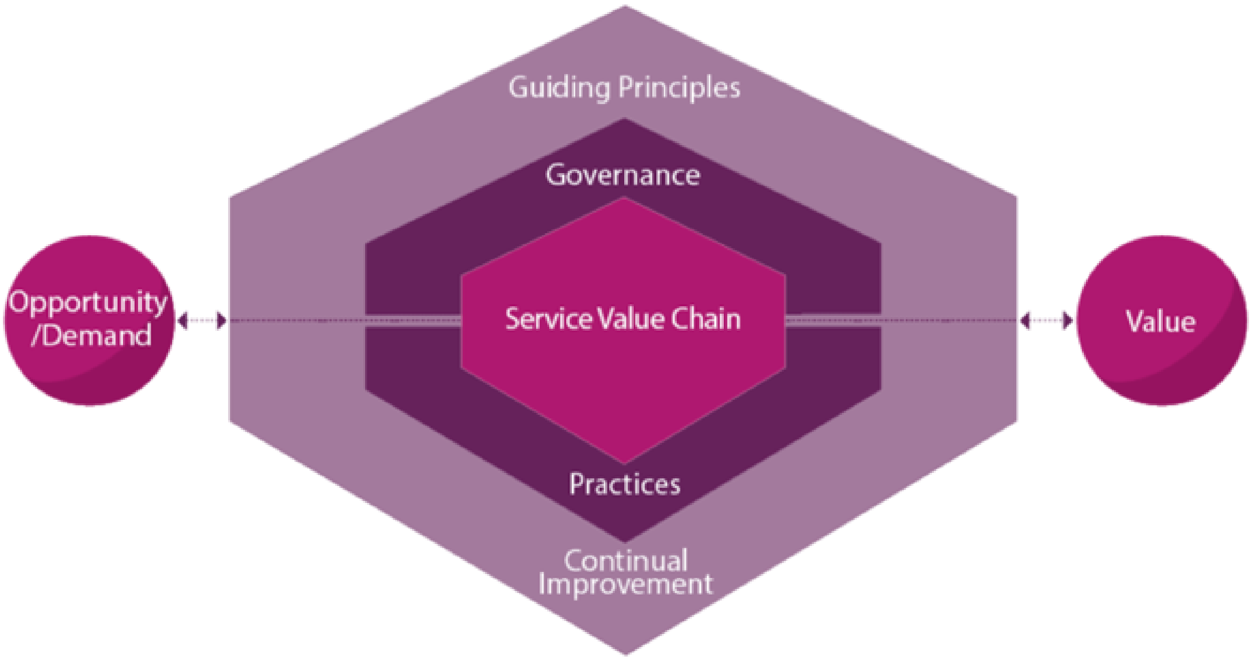


Figure 6. The ITILv4 service value system (Axelos 2019)

The diagram above displays the six key activities of the service value system: guiding principles, governance, the service value chain, practices and continual improvement. The service value system is flexible can be integrated in multiple different organizational approaches, the system also considers the changing demands of the company's stakeholders. (Axelos, 2019, p. 13-15)

The four dimensions model displays the dimensions by which the service value system should be applied. (Axelos, 2019, p. 13-15)

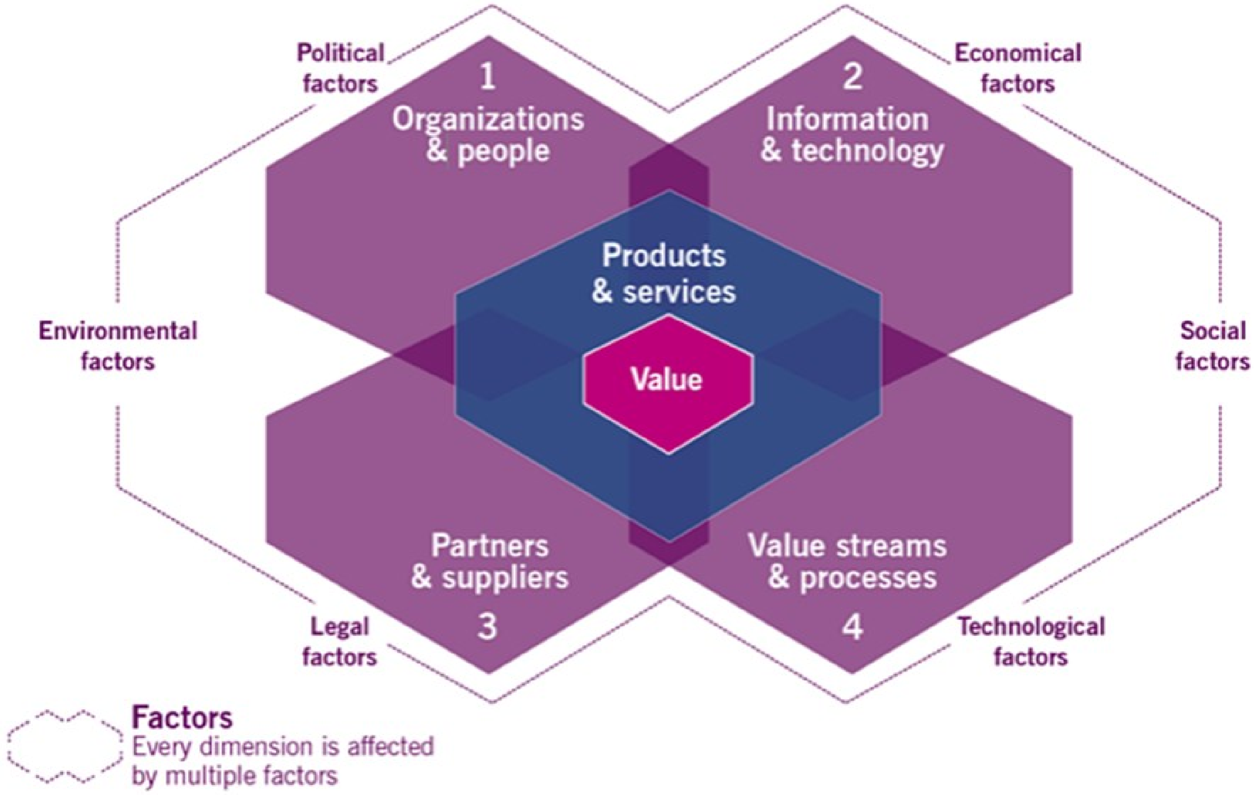


Figure 7. ITILv4 four dimensions (Axelos, 2019)

As can be seen in the figure above, the four dimensions are organizations and people, information and technology, partners and suppliers and value streams and processes. By applying equal amount of attention to each of the dimensions the service value system can be kept in a stable and useful condition. (Axelos, 2019 p. 13-15)

4.3.1 Information security management

The key purpose of information security management from the point of view of ITIL is for the company in question to understand and put into practice the concepts of managing confidentiality, integrity and information availability. Managing information security is done from three perspectives: preventative, detection, and correction. These perspectives should be appropriately balanced with the use of processes, policies, behaviors, risk management and controls. (Axelos, 2019) In order to properly establish practical information security practices, a functional identity and access management process should be in place as access management can be described as something that puts the policies defined in information security management into practice. (Malone, 2009, p. 75-78)

4.3.2 Access management

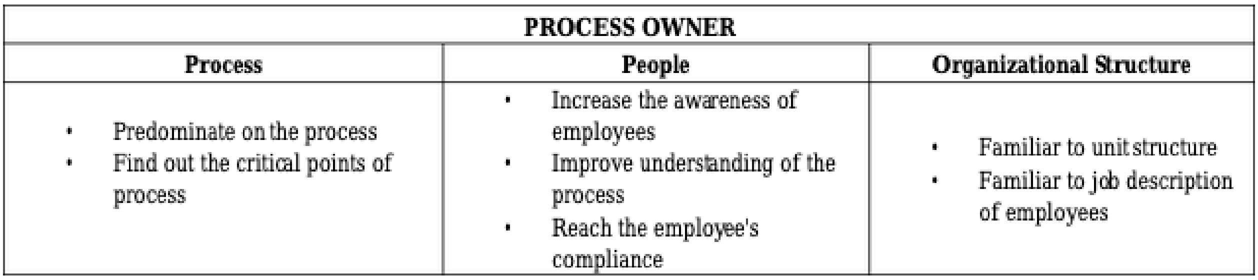
The main objective of access management is to enable authorized users to have access to the material they are authorized to access and to stop unauthorized users from accessing material that they shouldn't have access to. Access processes should also be integrated with existing business processes to ensure that the correct access tiers can be monitored, in conjunction to the users position in the organization. (Malone, 2009, p. 141)

Activities within the access management lifecycle include access requesting, verification, providing rights, monitoring identity status, logging and tracking access and removing or restricting rights. These activities can parallel activities in an identity's lifecycle, for example in the case of changes in position in the organization or in deprovisioning stage. (Malone, 2009, p. 141)

4.4 Process ownership

A process is a set of related tasks, which are done to achieve a business outcome. Often in organizations the role of a process owner exists alongside a process to ensure that the process is fulfilling its objective. A process owner is responsible for setting the goalposts of how the process should be performing and for improving the efficiency and performance of the specific process. A process owner also makes sure that the people interacting with the process possess the necessary knowledge, skills and tools. A process owner is responsible for every part of the specific process as their function is to ensure that the process is properly followed, the process design is efficient and to intervene when necessary to improve the process. It's important that the process owner has enough influence inside the organization to involve related parts of the organization in order to make changes if needed. (Larsen and Klischewski, 2004)

On a more practical level, in order to manage a process, it first has to be defined, which includes dividing the process into individual tasks and distributing them to each role involved in the process. Only after the process has been sufficiently defined, can measures for improving the process be put into action. Every process should have an owner; however, it should be kept in mind that a process owner doesn't necessarily mean a single person. A process can be owner or managed by example a small team instead of an individual. A lack of an identifiable process owner can lead to chaos. (Maddah and Hajiheydari, 2012)



PROCESS OWNER		
Process	People	Organizational Structure
• Predominate on the process • Find out the critical points of process	• Increase the awareness of employees • Improve understanding of the process • Reach the employee's compliance	• Familiar to unit structure • Familiar to job description of employees

Figure 8. Process owner interrelated concepts (Maddah and Hajiheydari, 2012)

In an organization a process owner often deals with three different aspects of process management displayed in the figure above: the process itself, the people involved in the process and the organizational structure which connects the people and the process. When dealing with the process itself the process owner should have command over it, identifying the different aspects of it on both a technical and operational level. With the use of various process analysis tools, a process owner can find where within the process value is created and therefore find the critical points of the process. When dealing with the people connected to the process, the process owner should increase the awareness of the employees and help them understand the process better. By growing the awareness and understanding of the employees, a process owner can more easily reach the employees compliance. When handling aspects of organizational structure, it is important that the process owner has authority and familiarity on the organizational structure and job descriptions of the employees. With a strong grasp and sufficient authority on the organizational structure, the process owner can make sudden decisions and maneuvers when necessary. (Maddah and Hajiheydari, 2012)

4.5 Conceptual data modeling

A conceptual data model is a presentation of organizational information requirements, which works as a way to communicate information between people in the organization in the process of determining and modeling information requirements. A conceptual data model combines application domain, data modeling and process knowledge to create a holistic view of the subject of the model. (Shanks, 1997)

The value of a conceptual data model can be measured from many points of view such as correctness, completeness, innovation, flexibility and understandability. Correctness in conceptual data models represents the amount of errors in the model, such as inaccuracies in entities and relationships. Completeness in this context represents how well the model supports user information requirements. Innovation in conceptual data models represents the new relevant and valid ideas that are introduced in the model. Flexibility in a conceptual data model implies the ability for the data model to consider changes without making changes to the model itself. Understandability represents how well the model communicates information to stakeholders in the data modeling process. (Shanks, 1997)

The abovementioned qualities are not the only features which determine the quality and usefulness of a conceptual data model. Oftentimes there are unknown qualities that are more difficult to pinpoint within the overall quality when comparing conceptual data models created by novices and experts. (Shanks, 1997)

4.6 Conceptual framework

The following diagram is a visualization of the conceptual framework for this thesis, which focuses on the logical progression of the thesis from the point of view of the literature review.

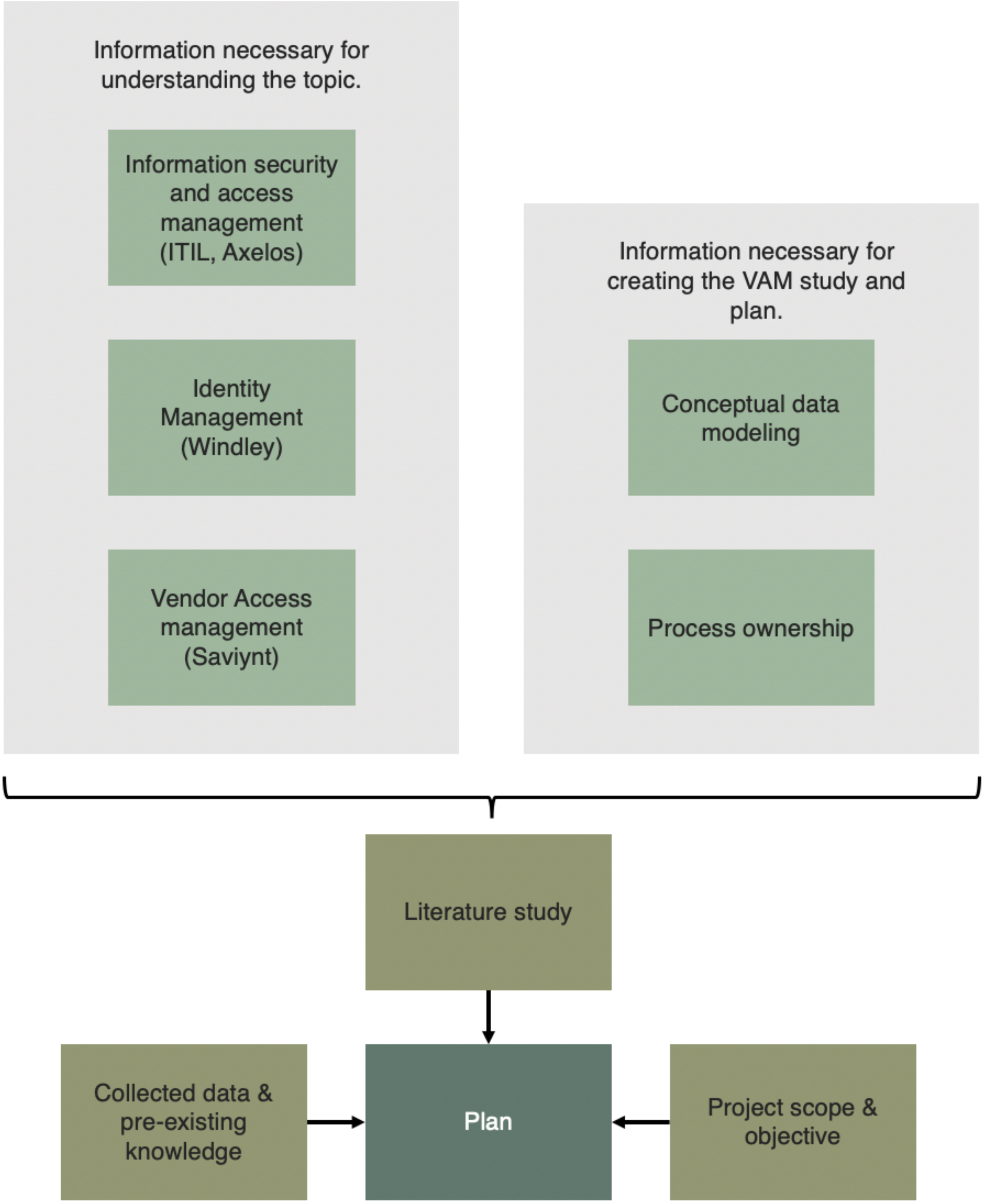

Information necessary for understanding the topic.
Information security and access management (ITIL, Axelos)
Identity Management (Windley)
Vendor Access management (Saviynt)
Information necessary for creating the VAM study and plan.
Conceptual data modeling
Process ownership
Literature study
Collected data & pre-existing knowledge
Plan
Project scope & objective

Figure 9. Conceptual framework

Starting from the upper half of the visualization, the key concepts of the literature review are displayed. On the left, there are the key concepts necessary for understanding the topic in a general sense. The concepts on the left side can be described as the literary foundation of the thesis, Identity management and vendor access management are the two key subjects outlining the thesis while information security and access management are related and important to the key themes of the thesis. On the right side of the upper half there are more specific areas of subject which are included in the key parts of the plan and VAM study. Process ownership is a point of interest in the plan as well as conceptual data modeling as the VAM study contains a conceptual data model. The components in the upper half of the diagram combine the knowledge needed to successfully formulate a plan from the literature point of view.

The lower half of the diagram displays the other key parts of the project including the literature review which are necessary for creating the plan, such as the scope and objective of the project and the collected and pre-existing data used to create the CSA and plan.

5 Plan building

In this section the results from the current state analysis and theoretical information and existing data are combined to create the first version of the plan. The plan building stage utilizes data from the second data collection point which consists of discussions with stakeholders and existing analysis with a focus on VAM studies and other components of the final plan.

5.1 Overview of the plan building stage

Data for the plan was collected through various workshops and discussions with the thesis advisor and other people relevant to the vendor access management process. The objective of the second data collection stage was to gain a clear understanding of what should be included in the plan, what aspects of vendor access management should be included in the plan and on what level.

The findings in the CSA indicate that the case company's vendor access management is mainly in a good position with most of the weaknesses being smaller and improvable and that the capabilities of the existing IdM system seem promising in terms of providing solutions to some of the weaknesses in the process. The CSA also provides points of focus in terms of weaknesses and strengths for building the plan.

The first step of the plan building stage was creating the VAM study which provides investigations in different aspects of architecture relating to the change. The VAM study includes explorations of the business, data, application and security architecture of vendor access management of how the architecture is in the desired state in the case company. To answer lack of accountability and focus in the vendor access management process, the plan is set to provide an analysis of the demand for a process owner and suggestions of who the process owner should be within the case company. To create a clearer view and a coherent understanding of the process within the company, the plan provides definitions for the key roles and points of interest within the process. Finally, the plan provides a proposal for how the vendor access management process should be conducted during the transitional stage of the HR systems.

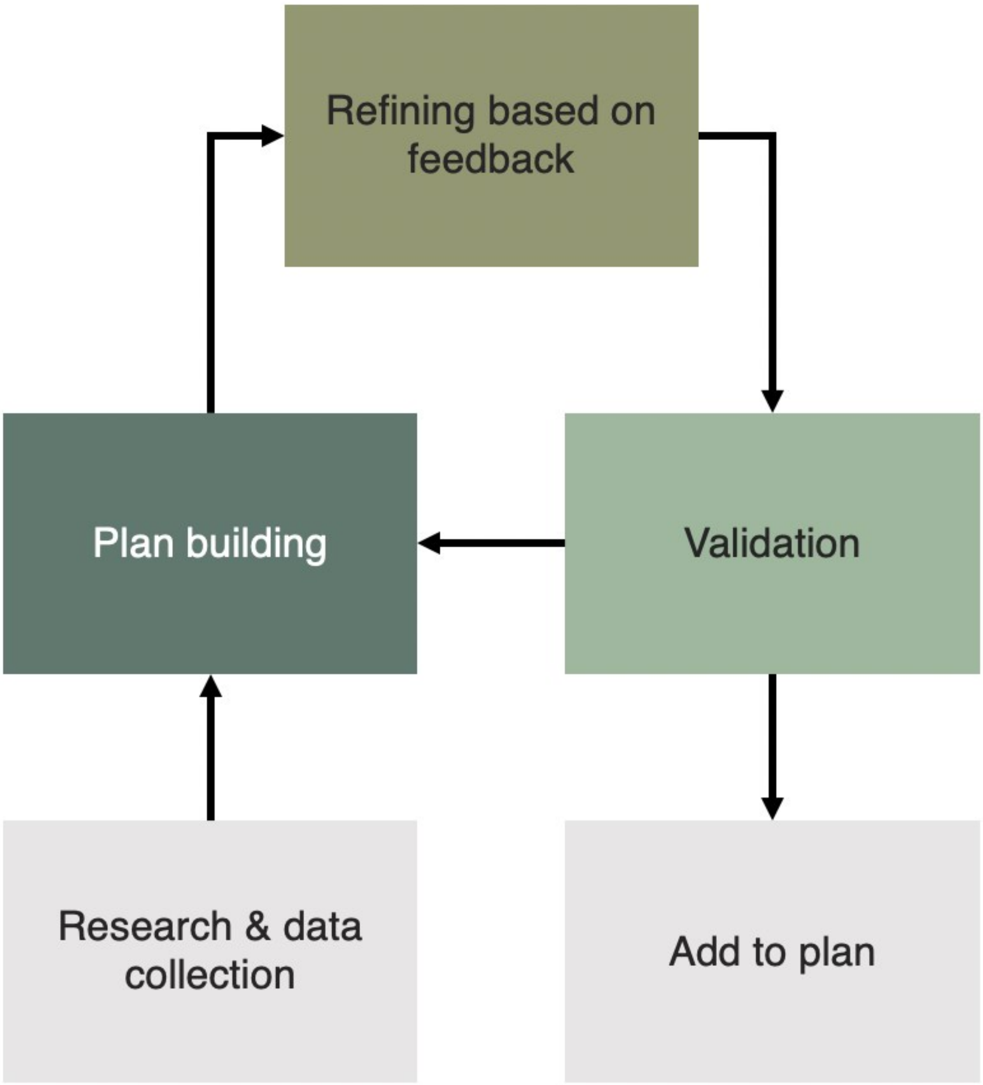


Figure 10. Plan building process

As can be seen in the figure above, the process for building each part of the plan was iterative with each section of the plan being refined and validated on a weekly basis.

5.2 Data collection 2 findings

The data gathered for the second data collection point consists of discussions consists of discussions and interviews with key employees within the case company, existing analyses and other VAM -studies relating to identity management.

The findings in the discussions showed that each of the separate parts of the VAM study should be conducted to create a thorough idea and background from which the case company can use as background material to forward towards the next steps in the progression of completely transferring the identity management of externals to the IdM system. The business architecture in the VAM-study displays the objectives of the vendor access management process from a business point of view. The data architecture consists of a conceptual data model, which is repurposed from the conceptual data model from the IdM process as it was found in the discussions that the two models would be similar in many ways. The application architecture displays the current IdM system and the all the other systems which surround and communicate with it. Also, in the discussions it was found that a logical data model might also be a useful addition to the study. The technology and security architecture in the VAM-study displays the security and technology utilized in the vendor access management process, however this section will be omitted from the thesis.

Both the literature study and the discussions showed that it is necessary for the vendor access management process to have a designated owner. Some of the weaknesses in the current state consists of and are related to the lack of decision making, direction and accountability in the process, all of these weaknesses can be improved upon by successfully appointing a process owner to take over the management of the process. When considering an owner for a process such as vendor access management, it is important to keep in mind that the process is related to multiple different parts of the organization such as sourcing and IT.

5.3 VAM study

As mentioned earlier the VAM study is a study which consists of various investigations in different aspects of architecture relating to the change with the objective of answering architectural questions related to GIT and enterprise architecture domains. The VAM study consists of four parts: business, data, application, security and technology architecture.

The process for building the VAM study varied significantly depending on the aspect of architecture. The process for building the architecture was a close collaboration with the thesis instructor as they had the accurate information about it. The data architecture consists of a conceptual data model which was created by modifying an existing model for the IdM process, a logical data model was considered but it was decided to instead display the more detailed flow of data between systems by creating a more detailed application architecture visualization. The application architecture consists of a three-part visualization of the application landscape of IdM, which shows the current, transition and target states. The technology and security section of the study consists of a brief overview of the security and technological side of the solution.

The process for building the architectures was iterative. A draft was first created, which was then reviewed in a weekly meeting and later improved upon until it sufficiently matched the needs of the project.

5.4 Process ownership

The lack of process ownership was one of the key points that came up in the CSA, which is why a proposal for the ownership of the vendor access management process is included in the maintenance plan.

The plan includes analysis based on the literature review and existing analyses to bring forth a suggestion for appointing an owner for the vendor access management process detailing the reasons and benefits while also suggesting where within the company should de ownership be located and why.

The basis for this suggestion is largely based on the literature review, weaknesses found in the CSA and a discussion within the IT department considering the various facets of process ownership in this instance.

*Same as with the VAM-study the process for building the suggestion was iterative, with each version reviewed and refined on a weekly basis.

5.5 Vendor access management definitions

The vendor access management definitions section of the plan includes definitions of various key concepts within the process, such as worker types, changes in the process and roles within the process.

Due to the organizationally wide reach of the vendor access management process, finding the appropriate definitions for the types of external workers was not a straightforward task. The discussions for determining the types were already in progress when the thesis was started. External workers in the case company have very different assignments ranging from IT consultants to production workers and cleaning staff, making it difficult to accurately define the types. With the process having broad significance, it was necessary to wait for the different parties within the company to come to an agreement in regard to the worker types. The section detailing the types is largely based on the discussions and agreements of the aforementioned parties.

The vendor access management definitions section also includes reviewing the IdM process in the different stages of IdM in the company, with the objective of finding out and detailing the possible changes in the process as the application landscape changes from the current state to the transition and target states.

Development in functionality in the IdM systems bring changes to the roles working with the IdM in bringing in new roles, such as the sponsor for an external worker, making it necessary to also pay attention to the roles within the process.

5.6 Transition stage

The transition stage section of the plan consists of several modified parts from the earlier sections, such as the application architecture visualization from the VAM-study. The purpose of creating the transition stage overview in the plan was to provide a clear image of which changes are feasible in a shorter period of time and to differentiate them from the long-term targets. For example, the HRMS system being replaced by an HCM system and reacting to the effects created by this change would be considered a change in the short term whereas opening the possibility of managing physical accesses within the IdM system would be considered as a change in the long term. Having a clear overview of the transition stage helps represent the changes in the IdM process in steps, which allows for a more straightforward execution of the coming changes in the systems.

Coming up with which parts of the process should be included in the transition stage overview is decided within discussions with the thesis supervisor where functional changes in the in the software and what is required to run the IdM process, as the changes are not yet completely implemented, are evaluated.

6 Plan validation

6.1 Validation process

The process for validating the plan was done in conjunction with the plan building process in an iterative manner as is shown in figure 10 above. What this means in practice is that smaller pieces of the plan were created separately and reviewed and refined with the thesis instructor on a weekly basis. The objective of this process was to make sure that that the contents of the plan are heading in the right direction and that errors are quickly corrected before they cause issues in later stages of building the plan while delivering an accurate and useful end product.

6.2 Data collection 3 findings

As the validation stage of the thesis was done piece by piece in an iterative manner the main changes based off of the third data collection points were often small but ultimately slowly changed the shape of the plan in a significant manner.

One of the changes that came up in the validation stage was to shift the focus of the challenges presented in the process ownership section towards the service contractor user type. The reason for making this change was to highlight the level of separation of the management of the service contractors from the other external worker user types and to point out how much the lack of ownership compromises the maintenance of these types of workers.

Many of the corrections done in the validation stage had to do with various logical corrections and clarifications in the conceptual data model and application landscape models. The models were modified time and again to ensure their accuracy and to make sure that they represent reality on the level that is necessary to move forward in the process of changing the IdM landscape in the case company.

Due to the constantly advancing process of slowly transitioning into the new systems, a lot of the terminology and user type names had to be changed during the validation process of the thesis. Oftentimes the changes in terminology were processed through multiple sections of the company before they were applied to the thesis. The reason for making these changes was to represent the processes accurately and to avoid confusion stemming from inconsistencies within the terminology-

It was also decided to leave the security and technology part of the VAM-study out of the thesis due to security reasons.

6.3 Final plan

This subheading consists of the final plan which is the product of the iterative plan building and validation process. The first section of the plan consists of the VAM-study, the second section provides suggestions in terms of ownership of the vendor access management process and the third part of the plan consists of definitions for the different external worker types.

The outcome of this thesis is meant to be used as background information for taking the next steps in terms of external workers in the different stages of the system changes within Vaisala in the coming months and years. The aim in terms of the contents of the plan has been selected based on the key demands and findings in the current state analysis

6.3.1 VAM study

This subchapter goes through the relevant parts of the VAM-study, starting from the business architecture. After business architecture the thesis looks at data architecture in terms of a conceptual data model and finally the chapter concludes with application architecture.

The following picture showcases the changes in terms of identities and the existing IdM system.

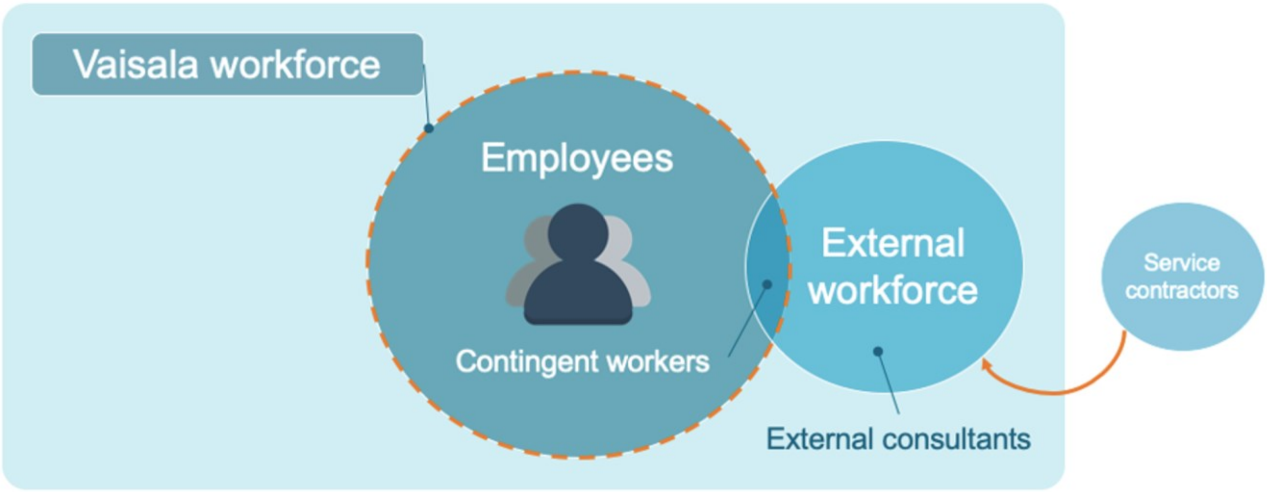


Figure 11. IdM workforce overview

In the current state the maintenance of employees and the external workforce is carried out in the HRMS. In the future employees and a part of the contingent workers will be maintained in the HCM system, whereas the majority of the external workforce will be managed within the IdM system. Service contractors have been managed completely outside of the identity management process, with the only systems they are in contact with being the PACS and ACMS systems. In the future the Service contractors should also be included within the maintenance reach of the IdM system. Adding service contractors to the scope of the IdM will significantly improve the security and increase productivity as the responsibilities and information about them will reside in the same location as where their maintenance will be performed.

The existing IdM system has capabilities for more robust vendor access management functionalities, which are to be designed and set up in the system in the future. User lifecycles will also have to be defined for the users that will not be imported from an external source system to the IdM system.

The following diagram is a conceptual data model detailing the external workforce.

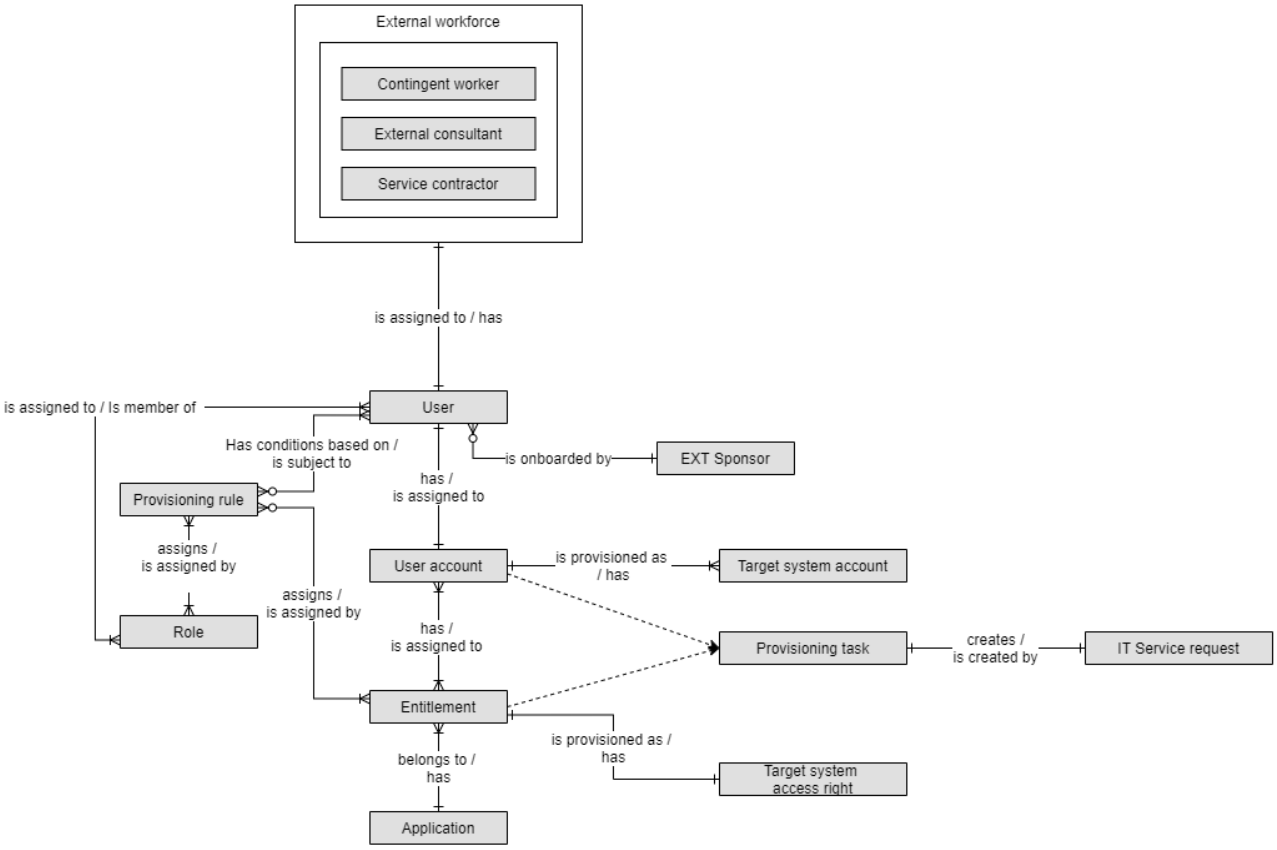


Figure 12. Conceptual data model

The conceptual model is largely similar to an employee's in terms of user attributes with the exception of the lack of a supervisor and the inclusion of the EXT sponsor. In the beginning of an external user's lifecycle, they are onboarded by an EXT sponsor, even though the existence of a supervisor in this case is not prohibited, it was still left out of the model as it's not necessary. As the design and functionalities of the IdM system in terms of the field of these features are still yet to be decided upon and comprehensively explored, this model is due to change as more knowledge is attained.

The following figure displays the application landscape in terms of identity management within Vaisala in the current state.

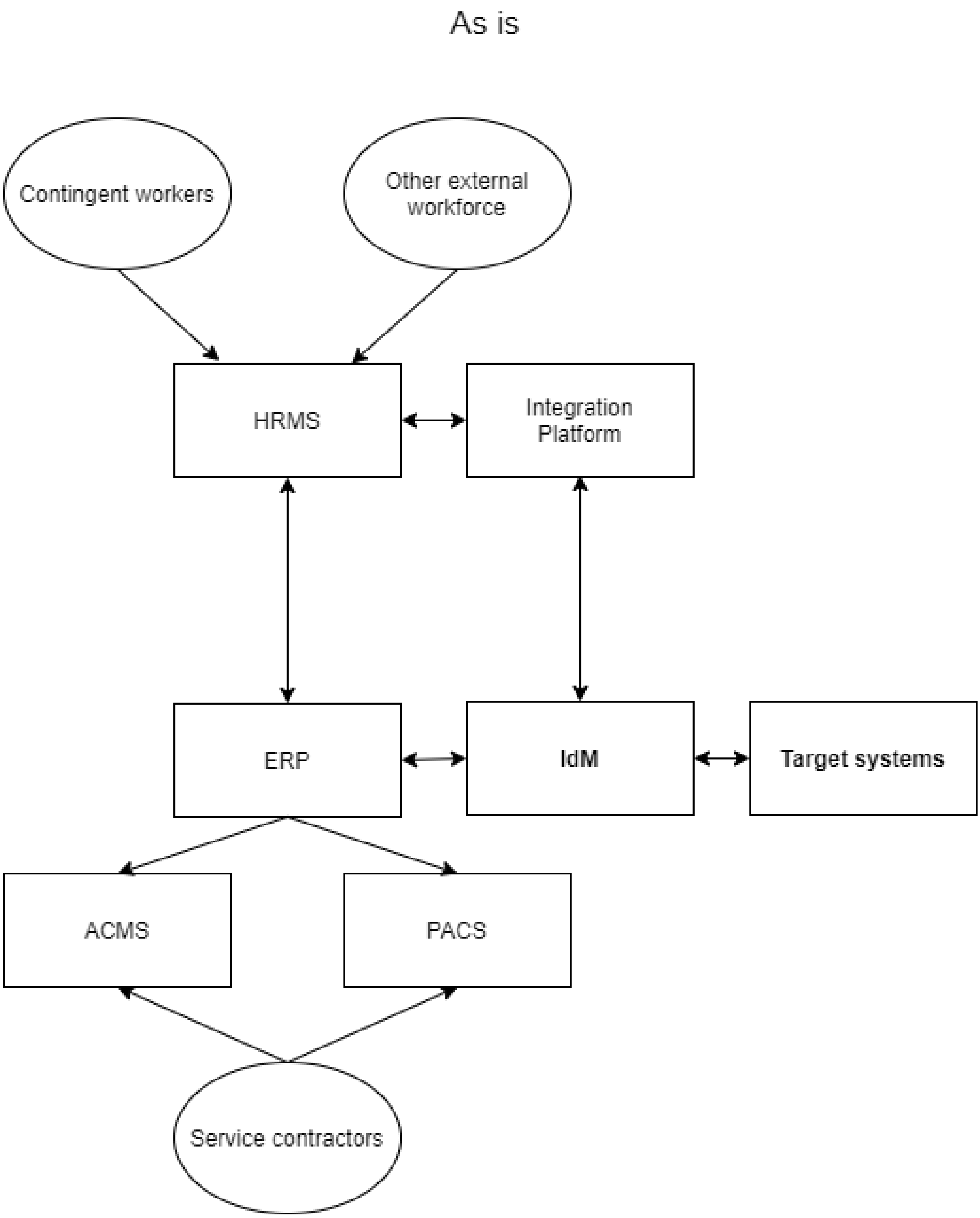


Figure 13. Application landscape current state

At the current state contingent workers and external consultants are managed within the HRMS which communicates with the ERP and the IdM systems through an integration platform, while the IdM system communicates and grants accesses to target systems.

Service contractors at the current state are only managed via ACMS and PACS systems completely externally from the IdM process.

The following figure displays the application landscape in terms of identity management within Vaisala in the transition state.

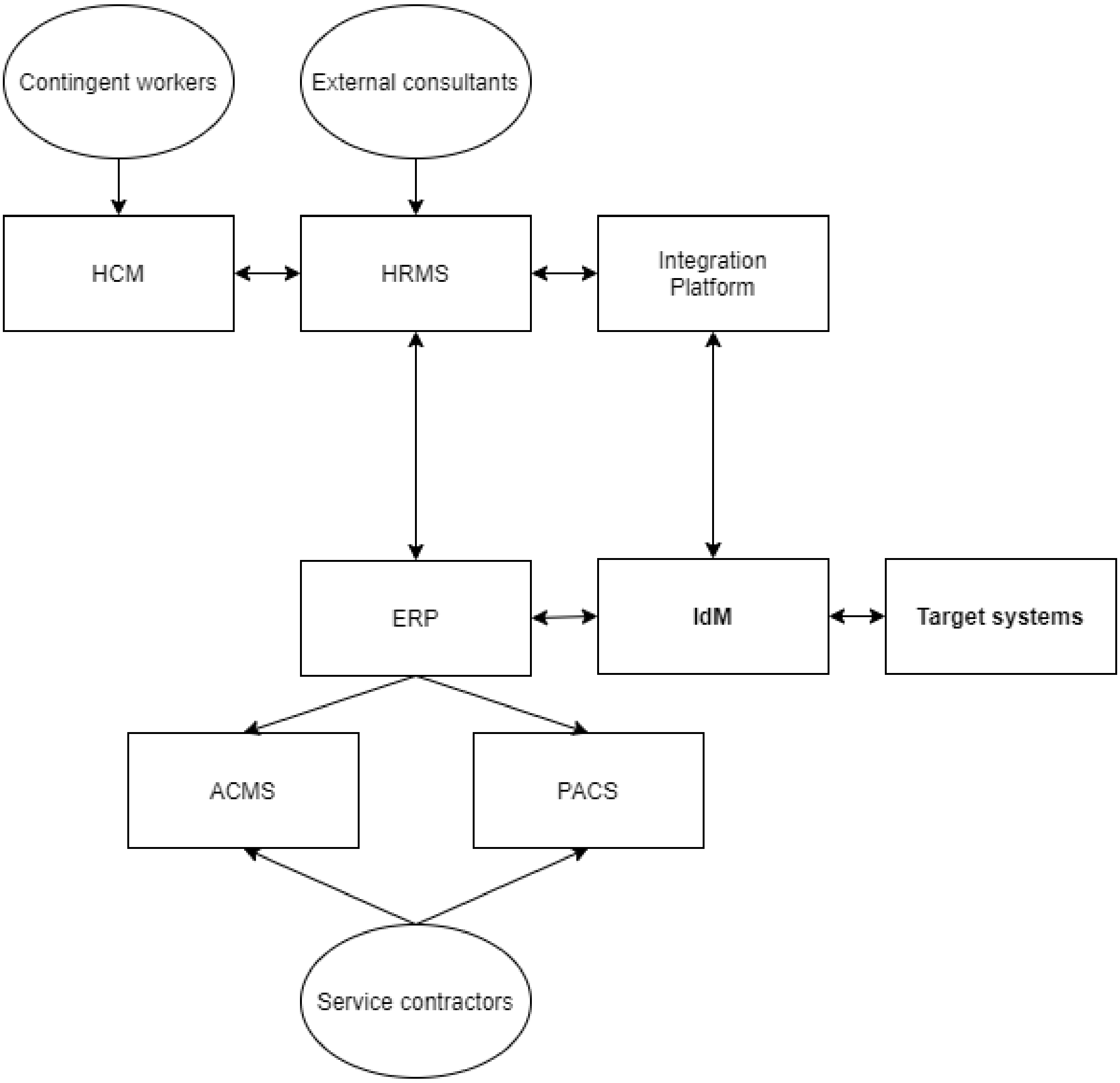


Figure 14. Application landscape transition state

During the transition stage the management of the contingent workers has been moved to the HCM system, while the identities of external consultants are still sourced from the HRMS to the IdM system through the integration platform. The management of Service contractors is still the same in the transition state and the current state.

The following figure displays the application landscape in terms of identity management within Vaisala in the target state.

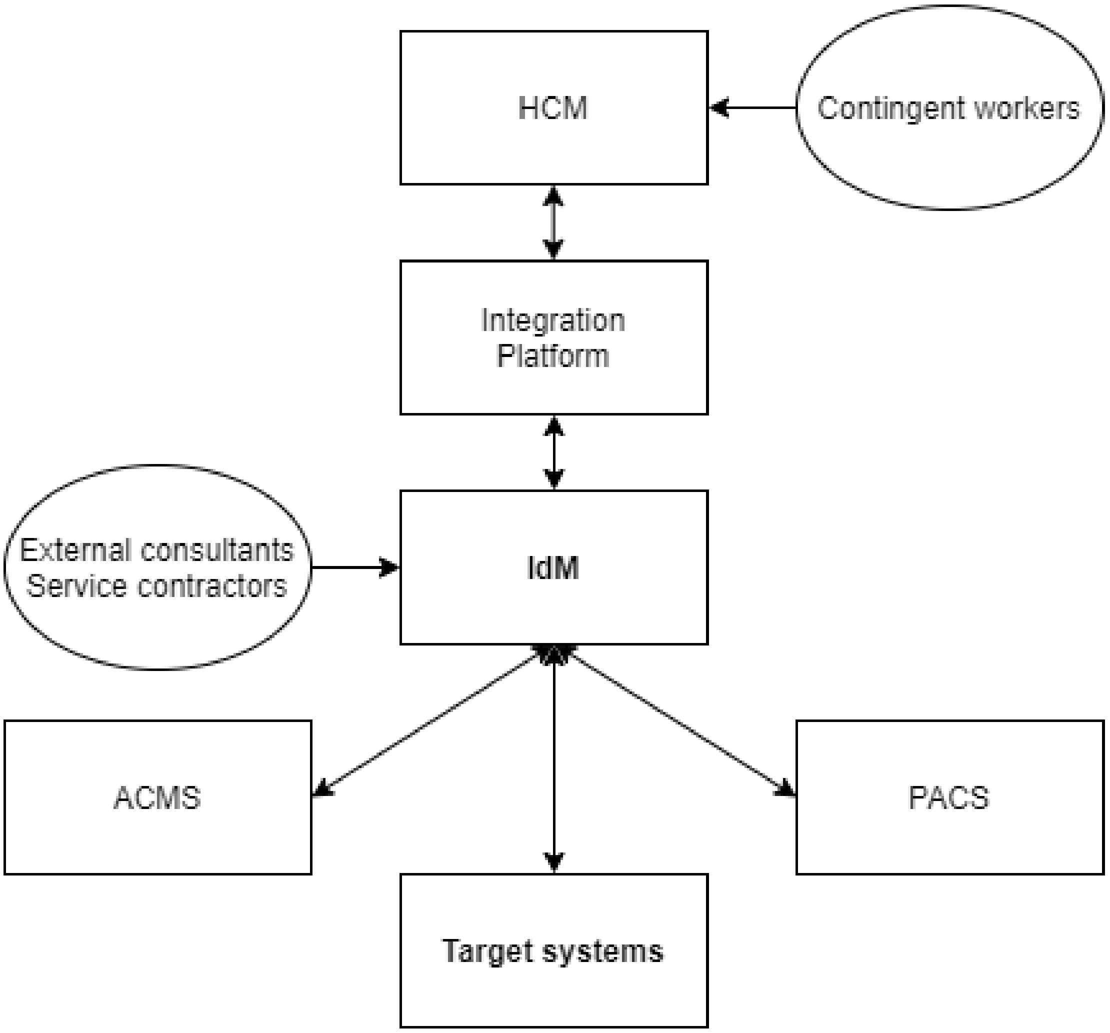
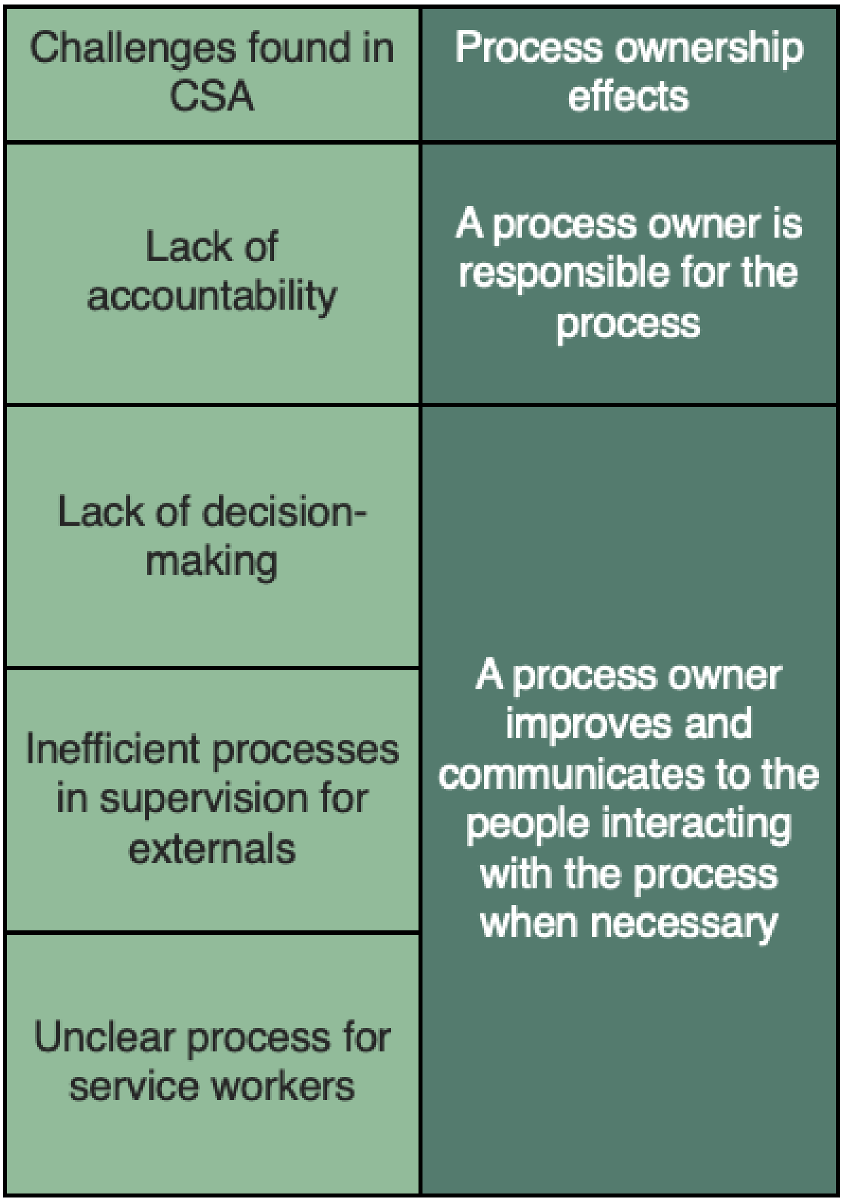


Figure 15. Application landscape target state

In the target state contingent workers are managed within the HCM system which communicates with the IdM system through the integration platform. Both external consultants and service contractors are managed within the IdM system without the use of an external source system. In the target state both the ACMS and PACS systems communicate directly with the IdM system and not the ERP.

6.3.2 Process ownership

Many of the issues that came up in the findings of the current state analysis have to do with the vendor access management lacking in direction, accountability and leadership, which causes a lack of clarity and progress when it comes to developing the process further. All of the aforementioned issues are mainly apparent in the case of service contractors and are caused by a lack of process ownership. In the current state the maintenance of the service contractors is completely the responsibility of facilities in Vaisala. While studying the literature, it became apparent that appointing a specified owner to a process and introducing a broader scope of external workers to the process would strengthen the process and create and entity which is responsible for the direction, efficiency and functionality of the process. The figure below demonstrates the comparisons of the weaknesses in the process and the effects of process ownership.



Challenges found in CSA	Process ownership effects
Lack of accountability	A process owner is responsible for the process
Lack of decision-making	A process owner improves and communicates to the people interacting with the process when necessary
Inefficient processes in supervision for externals	
Unclear process for service workers	

Figure 16. Process weaknesses and process ownership effects comparison

Due to the way that appointing a process owner for the vendor access management process would answer to the issues found in the CSA, it is necessary to find and appoint a person or a team to govern over the process to ensure that the process performs at the expected level.

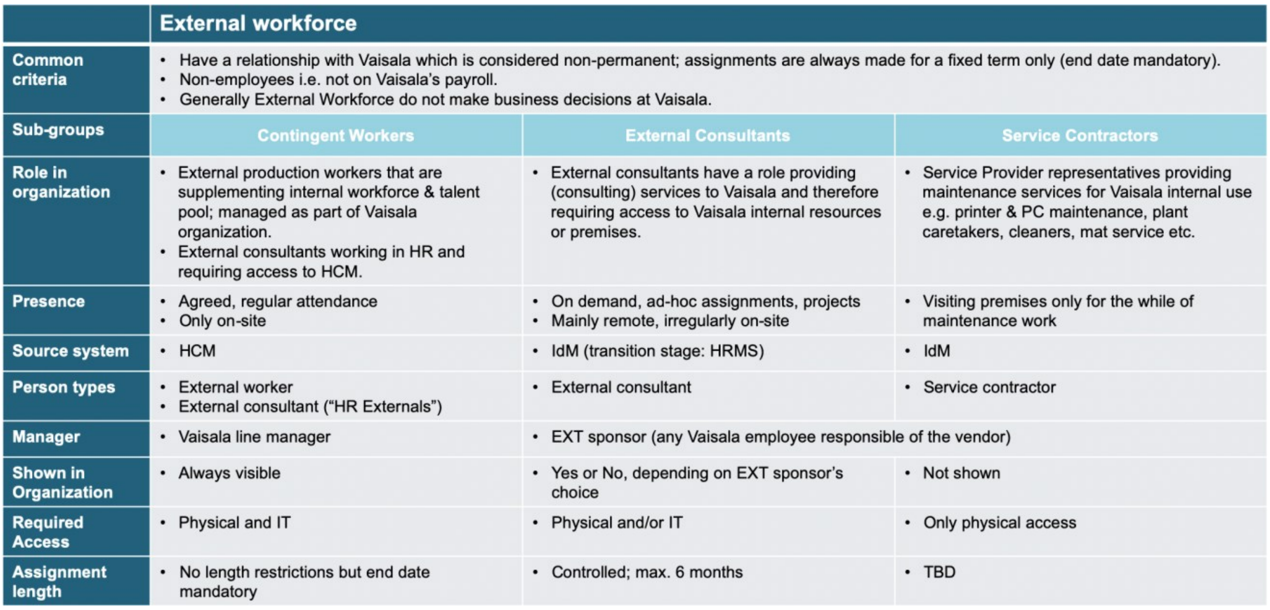
The issues that come about when deciding who should have ownership of the process are related to its long reaching influence throughout the company. Vendor access management as a process within Vaisala is in contact with for example IT, HR, security and sourcing departments, which makes it important to have a clear view of who would be most suitable to take the position of the process owner.

At the current state, the IT department is the owner of the access management process in its entirety. While the vendor access management process is performed by various different departments within Vaisala it would be the most logical conclusion that the process would be owned by the IT departments as the access management process considers many of the same matters as the vendor access management process.

6.3.3 Vendor access management definitions

Vendor access managements is the process for managing the external workforce from third party vendors throughout their lifecycle from onboarding to deprovisioning while minimizing non-employee risks with the use of internal EXT sponsors and external organizations.

The external workforce within Vaisala consists of contingent workers, external consultants and service contractors from third party service provider. All of these worker types have fixed term assignments and are not on Vaisala's payroll, having an end date for external workers is mandatory. A detailed breakdown of the criteria and characteristics of the different types can be viewed in the figure below.



	External workforce		
Common criteria	• Have a relationship with Vaisala which is considered non-permanent; assignments are always made for a fixed term only (end date mandatory). • Non-employees i.e. not on Vaisala's payroll. • Generally External Workforce do not make business decisions at Vaisala.		
Sub-groups	Contingent Workers	External Consultants	Service Contractors
Role in organization	• External production workers that are supplementing internal workforce & talent pool; managed as part of Vaisala organization. • External consultants working in HR and requiring access to HCM.	• External consultants have a role providing (consulting) services to Vaisala and therefore requiring access to Vaisala internal resources or premises.	• Service Provider representatives providing maintenance services for Vaisala internal use e.g. printer & PC maintenance, plant caretakers, cleaners, mat service etc.
Presence	• Agreed, regular attendance • Only on-site	• On demand, ad-hoc assignments, projects • Mainly remote, irregularly on-site	• Visiting premises only for the while of maintenance work
Source system	• HCM	• IdM (transition stage: HRMS)	• IdM
Person types	• External worker • External consultant ("HR Externals")	• External consultant	• Service contractor
Manager	• Vaisala line manager	• EXT sponsor (any Vaisala employee responsible of the vendor)	
Shown in Organization	• Always visible	• Yes or No, depending on EXT sponsor's choice	• Not shown
Required Access	• Physical and IT	• Physical and/or IT	• Only physical access
Assignment length	• No length restrictions but end date mandatory	• Controlled; max. 6 months	• TBD

Figure 17. External workforce criteria and characteristics

A contingent worker is in most cases a production worker who supplements Vaisala's internal workforce and is managed as a part of the Vaisala organization. An external consultant in the HR department who requires IT access is also a part of this category. Contingent workers are managed by Vaisala line managers and are always visible in the organization chart. The identity management of contingent workers is carried out in the HCM.

An external consultant provides consulting services to Vaisala and requires physical and/or IT accesses. These types of workers usually work on ad-hoc assignments and projects mainly remotely. An external consultant is managed by an EXT sponsor, a Vaisala employee responsible for the vendor who also decided whether or not the consultant is visible in Vaisala's organization chart. The identity management for external consultants is produced in the HRMS during the transition stage and in the IdM in the target state.

Service contractors provide maintenance services, such as printer & pc maintenance, plant care and cleaning services for Vaisala. Service contractors are also managed by EXT sponsors; however, they are not shown in the organizational chart. Service contractors require physical accesses to the Vaisala office premises but never any IT accesses. The identity management for the Service contractors is carried out within the IdM in the target and transition states.

Implementing a new way of maintenance for the external workforce will require defining roles and entities such as EXT sponsor, organization and organization owner. Unfortunately, due to time and scheduling constraints with stakeholders those definitions were not included in this thesis as it was decided in a conversation with the project advisor that more information is required about them from stakeholders to properly define them.

7 Thesis overview

7.1 Executive summary

The objective of the thesis was to create a plan which addresses three different stages of the identity management of the external workforce during the coming changes in the application landscape in Vaisala from the point of view of data modeling, application landscapes, process ownership and user definitions.

The thesis began with an analysis of the current state of the external workforce from the perspective of identity management. The data for the analysis was procured from discussions with the various stakeholders and from existing documents from the case company. The key outcomes from the current state were the overview of the coming changes, the current application landscape from the point of view of identity management and the overview of strengths and challenges in the current state of vendor access management in Vaisala that would need to be addressed within the thesis.

The literature research was conducted with an emphasis on identity and vendor access management in addition to exploring the different subjects used in the plan such as process ownership and data modelling. By utilizing the results of the literature study combined with the current state analysis and the objective of the thesis, the process for building the plan was started.

The plan consists of two major sections, the VAM-study and the separate sections supplying the points of view that the VAM-study does not address. The key outcomes of the plan were the conceptual data model for the target state of the vendor access management process, the application landscapes detailing the changes in each of the different parts during future developments in vendor access management within the case company, the exploration of the need for a process owner and what benefits would appointing one have and finally an overview of the characteristics of the external workers within the process in the target state. The plan was validated and reworked with the thesis advisor in the case company to ensure the accuracy and direction of the contents of the plan.

7.2 Next steps

The outcomes of the plan building and validation stages can be used stepping stones to develop IdM in the case company further and as a tool for moving forwards towards the upcoming system changes that inspired the creation of this thesis. The models are to be used as a starting point for beginning the development of the new IdM processes.

For the next steps in progressing towards the system changes, the case company should spend time further exploring the intricacies of the new entities and functions brought in by the changes and further utilization of the IdM system in full detail with the help of the supplier of the system.

After more robust information about the functionalities of the IdM system in terms of vendor access management are procured, the now roles and entities within the process should be defined to appropriately match their position within the process and while taking into account the maintenance of the process.

To ensure that the vendor access management process runs at the expected level and to account for the issues found in the process in the CSA, the case company should appoint a process owner for the vendor access management process. During the plan building stage, it became apparent that the process should be governed within the IT department.

All of the outcomes created during the thesis are made to be developed and customized through usage, post evaluation and continuous improvement.

8 Conclusions

8.1 Thesis Evaluation

The initial objective of the thesis was to build a plan to prepare the case for the upcoming system changes from the point of view of vendor access management. While creating the thesis, the scope of the thesis became more defined and clearer as more and more information emerged. The initial objective was mainly achieved as the thesis produced a plan for how to tackle application landscape changes, conceptual data model changes and other adjustments within the process of vendor access management during the system changes. All of the information presented in the theory was necessary and was utilized in the plan in some manner. Unfortunately, the area of process maintenance was addressed on a smaller scale than planned, this was due to scheduling issues with the parties necessary to create a more robust view of that phase of the process.

The thesis successfully followed the research design framework displayed in chapter 2. Each of the data collection points, outcomes and thesis stages were utilized as planned in the framework.

Due to active communication and collaboration with the case company, staying ahead of the schedule was possible. Outcomes were delivered according to the deadlines set by the case company and thesis author.

The data collection in the project was sufficient for reaching the desired outcomes. The data was mainly gathered in the form of meeting notes and by utilizing the pre-existing documents from the company.

In some parts of the thesis building process, there were some issues in terms of the focus shifting between process improvement and plan building, but ultimately these issues were addressed, and the thesis was adjusted as necessary, resulting in a concise and cohesive body of work.

One of the goals in creating this thesis was making sure that the outcomes created are valid, reliable and useful for the case company. The reliability of the outcomes was strengthened first by taking a wide aspect of viewpoints and relevant sources of information to base the study off of. During the process of writing the thesis continuous feedback and validation was gathered from the thesis advisors both within the case company and Metropolia UAS. The validity of the outcomes was established by first creating the current state analysis to understand the vendor access management process in the current state to have a good grasp of the challenges and needs of the process moving forward. The thesis was created in close collaboration with the project advisor in the case company, who supplied guidance, information and continuous feedback during the creation of the thesis strengthening its validity.

References

Windley, P., 2008. Digital Identity. Sebastopol: O'Reilly Media, Inc.

Al-Khouri, A., 2011. Optimizing Identity and Access Management (IAM) Frameworks. International Journal of Engineering Research and Applications, 1(3), pp.461-477.

Saviynt, 2020. Saviynt For Vendor Access Management Comprehensive Solution For Identity Governance. [online] https://saviynt.com/. Available at: <https://saviynt.com/solution-guides/saviynt-for-vendor-access-management/> [Accessed 23 November 2020].

Axelos, 2019. ITIL Foundation. London: The Stationery Office Ltd.

Malone, T., 2009. ITIL V3 Foundation Complete Certification Kit.

Larsen, M. and Klischewski, R., 2004. Process Ownership Challenges in IT-Enabled Transformation of Interorganizational Business Processes.

Maddah, M. and Hajiheydari, N., 2012. The Role of Process Owner on BPM-System Implementation Success.

Shanks, G., 1997. Conceptual Data Modelling: an empirical study of expert and novice data modellers. Australasian Journal of Information Systems, 4(2)