SAVONIA

THESIS – BACHELOR'S DEGREE
TECHNOLOGY, COMMUNICATION AND TRANSPORT

STAKEHOLDER PERSPECTIVE IN IDENTITY AND ACCESS MANAGEMENT

Identifying key IAM requirements through stakeholder analysis in a manufacturing company

AUTHOR Iiris Hare

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport	
Degree Programme Degree Programme in Information Technology	
Author Iiris Hare	
Title of Thesis Stakeholder perspective in Identity and Access Management - Identifying key IAM requirements through stakeholder analysis in a manufacturing company	
Date 12.12.2025	Pages/Appendices 34/1
Client Organisation /Partners Manufacturing organisation X	

Identity and Access Management (IAM) plays a critical role in safeguarding company data by ensuring that the right users, machines and software components have appropriate access at the right time. Identity Management (IDM), a key subdomain of IAM, provides the interface for managing the entire lifecycle of user identities and their access rights. This thesis was conducted in collaboration with a global manufacturing company. Manufacturing environments demand strict access control due to high automation and hazardous conditions. In such environments, effective IAM plays a critical role in ensuring operational safety and continuity. The aim of this thesis was to identify intensive IAM stakeholders in the company, explore their expectations and values, and assess how current IAM solutions on the market meet their needs.

The research was conducted as a case study which combines both qualitative and quantitative data. First, stakeholders were identified through an IAM report highlighting users with the highest number of requests. Next, a structured survey was distributed to these stakeholders, and finally the responses were analysed and compared against three selected IAM solutions. Additionally, three persons presenting different fields were interviewed to gain a deeper understanding of IAM practices and perspectives. Their insights were incorporated to support the survey findings and provide additional detail to this research.

The results show that IT, Operations, Finance, and HR were the primary stakeholder groups actively using IAM system in the Company X. The responses were largely consistent among them. Stakeholders place the highest value on a clear and intuitive user experience, fast and reliable access provisioning, and strong security and data protection. When asked about the most anticipated benefits of a future solution, they highlighted the importance of automation, improved visibility of roles and seamless integration to critical organisational systems. IAM experts emphasised that the system should be modular to meet modern standards and potentially leverage AI.

For further research, it could be interesting to expand the study to include the stakeholders who are not intensive users but are still affected by actions from IAM or contribute to IAM operations, as they were completely excluded from this research. This thesis serves as an initial investigation by identifying key expectations across departments and offers both practical and strategic value for the commissioning organisation. The study provides a foundation for defining IAM system requirements, and its insights can hopefully support decision-making and foster collaboration across departments. Future research could take a more detailed and technical approach to further develop these findings at a practical level. For the researcher, the thesis has been significant for professional development.

Keywords
IAM, IDM, IGA, stakeholders, manufacturing industry, digital identity

CONTENT

LIST OF FIGURES

1 INTRODUCTION

Identity and access management (IAM) has a big role in protecting enterprise environments from threats coming from inside and outside. It ensures that the right users, machines, and software components have the right access at the right time through their entire life cycle. Selecting an IAM system that aligns with the company's specific needs enhances security and overall organisational efficiency: it streamlines user access, reduces administrative overhead and related costs, simplifies processes and lets employees work without unnecessary delays or technical barriers. In contrast, a poorly functioning IAM system can introduce vulnerabilities, increase the risk of human error, and frustrate users with access issues and slow response times.

This thesis is a stakeholder-driven analysis to better understand what different actors value in identity and access management and how those insights can inform system requirements in the context of global manufacturing business. The focus was identifying the key stakeholder groups interacting with identity and access management (IAM) systems, understanding their needs, and uncovering their expectations for these systems. Research was implemented by collecting data with a structured questionnaire and by interviewing selected participants to gain deeper insights into specific themes. The findings from both the survey and interviews were used to define the key requirements for an IAM system in a manufacturing organisation and compared against selected existing IAM solutions to evaluate how well they align with stakeholder expectations.

Thesis was done in cooperation with a global manufacturing business, later referred as Company X. In industrial settings – such as manufacturing plants, underground facilities, or environments involving high temperatures and hazardous machinery – controlled access is critical. IAM systems support secure access to production environments and ensure compliance with regulations. However, the effectiveness of these systems depends not only on technical features but also on how well they align with the expectations and needs of various stakeholders. This study provides a foundation for defining system requirements that are coming from real operational demands. These insights can hopefully support the decision-making in future system evaluations and foster a dialogue about the effectiveness of current practices and highlight areas for improvement.

2 IDENTITY AND ACCESS MANAGEMENT

Identity and Access Management (IAM) is a key component of organisational cybersecurity. It regulates how users – such as internal employees, external contractors, and business partners – access the company technology and infrastructure. At the core is ensuring that each user has exactly the access they need for their role, no more, no less (Cloudworks n.d). As roles evolve due to promotions, absences, or new responsibilities, these changes must be accurately reflected both in IAM and access rights.

When organisations began to recognise the increasing complexity of managing user access across multiple systems in the late 1990s, the concept of IAM started to gain recognition. At the time, user access had to be updated manually for each system, making maintenance both challenging and time-consuming. By the early 2000s, IAM practices were gradually integrated into enterprise tools and platforms, becoming a strategic part of IT infrastructure and governance (Skypro AG 2024).

IAM helps keeping widely spread and complex resources in control. In modern organisations, where systems span across cloud services, on-premises environments, and third-party platforms, IAM provides a centralised way to manage identities and reduces the risk of unauthorised access. In the past, securing company resources behind a firewall was sufficient, as employees worked on-site and could access systems simply by logging in. Today, with hybrid work becoming more common, secure access has become critically important to ensure data protection across diverse environments (Microsoft 2025).

2.1 Interconnected aspects

As seen in the figure 1, Identity Governance and Administration (IGA), Identity and Access Management (IAM) and Identity Management (IDM) are interconnected aspects that together form a comprehensive framework for managing user identities and access rights. At a high level, Identity Governance ensures that Identity and Access Management follows the organisation’s policies and compliance requirements. IAM brings together key elements such as account management, authentication, authorisation and different access control models, all governed by policies and access rules. Identity Management instead focuses on implementing these policies through lifecycle management which means creating, updating, and removing user accounts as roles change or employment ends.

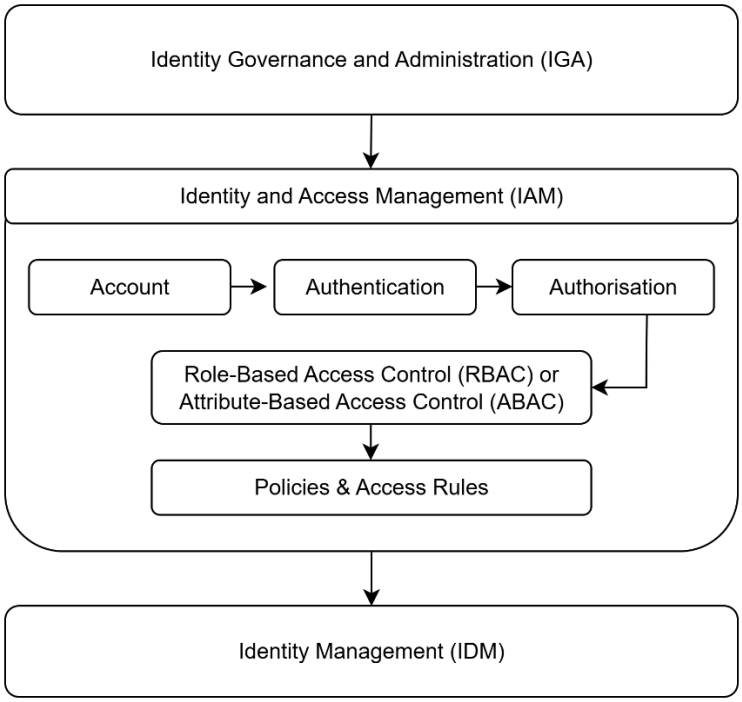

Figure 1. IGA, IAM and IDM are interconnected aspects

IGA is a framework and set of security solutions that are made to mitigate the identity-related access risks within the organisation. IGA automates the account management for individual users in an organisation. (Fortra 2020). While IAM can be seen as the door that grants access to users with the correct credentials, IGA acts as the gatekeeper: it regularly verifying whether those users should continue to hold access rights based on their roles, responsibilities and organisational policies.

Authentication is a process that validates the user identities by asking “Who are you?”. The authentication process is always tied to a specific account, which represents the digital identity of the user within the system. Digital identity, known also as user identity, is a collection of unique identifiers consisting of attributes like email, sign-in credentials, IP and MAC address, that are used to verify who the user, software or machine is, and to determine what they are allowed to access within digital environments (Microsoft Ignite 2025). User typically signs in using multi-factor authentication (MFA), confirming the identity with credentials such as a username and password. (Tenable 2025)

Authorisation is a process that asks the user “Where do you have access and what can you do there?”. A common access control model is *Role-based access control (RBAC)* which grants permissions based on roles such as “networking specialist”, “developer” or “HR manager”. Role management defines which permissions each job function should have: for instance, a production engineer may be granted access to process control systems and maintenance records, while being restricted from financial reporting tools. The other approach, *Attribute-based access control (ABAC),* is more flexible but also more complex approach that uses a combination of attributes, like job title, department and location, to evaluate the access policies. (Tenable 2025)

Access rules define logic that governs authorisation decisions: they specify the conditions under which access is granted or denied. For instance, a user who is an internal employee and belongs to the finance team may be granted a particular role with its associated entitlements. *Policies*, on the

other hand, operate at a higher level: they define who can perform which actions on which resources and under what circumstances (Tiny Technical Tutorials 2021). In essence, rules are the technical implementation of policies. Policies ensure that access is aligned with organisational requirements including security standards and contextual constraints such as time, device or location.

2.2 Identity management (IDM)

Identity Management (IDM) is a key subdomain of IAM and created to manage identity-related data for company's workers and partners. IDM system serves as a user interface for administering the entire lifecycle of user identities and their access rights from creation to modification and finally to deactivation. As these systems manage not only identities but also access rights, they are nowadays considered part of IAM systems. However, the terms IDM and IAM are easy to confuse and are often used as synonyms.

Figure 2 shows how IAM systems are typically synchronised across multiple systems to ensure consistency and security. They can be interacting with HR system, Entra ID, Active Directory and different business applications such as SAP (System Applications and Products in Data Processing). In addition to the production environment, IAM systems may also include a dedicated Quality Assurance (QA) environment which is used for testing purposes, allowing new configurations, updates and integrations to be validated before deployment to production.

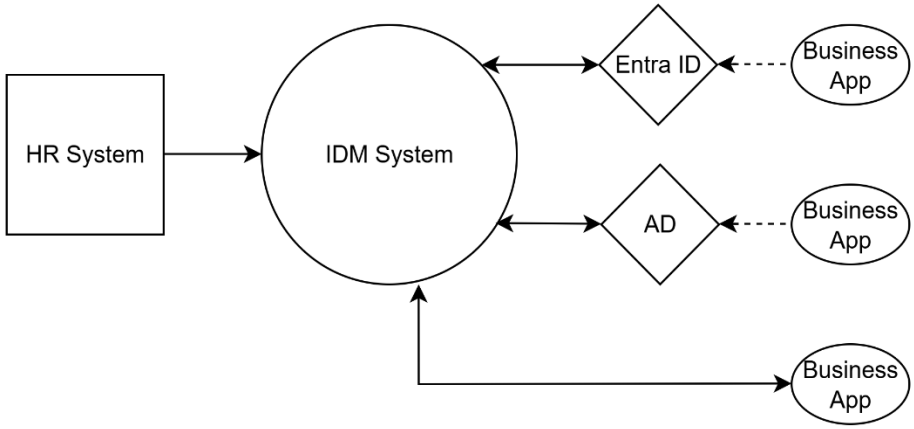

Figure 2. IAM system interacts with various systems. Adapted from Kotilainen 2024

IAM system interacts closely with *Human resources (HR) system*. The HR system manages employee records and the organisational structure, serving as a key source of master data. This master data typically includes employee's name, job title, department, location, supervisor, and employment status, which are essential for IAM and other business processes. In many organisations, internal employees are first created in the HR system, which then triggers automated provisioning processes in the IAM system. This means that user accounts are generated and assigned appropriate access rights across the IT environment. External identities, such as contractors or partners, are typically managed directly within IAM system, as they are not part of the HR system.

Active Directory (AD) is Microsoft's on-premises directory service used to manage users, groups, and access within Windows environments (Awati, Chai & Gillis 2025). It plays a central role in authentication and authorisation and is commonly integrated with IAM systems for provisioning and access control. For example, when a role is assigned through an IAM system, it is typically translated into specific access rights, called entitlements. In practice, these entitlements often take the form of membership in different AD groups. Each AD group gives access to certain systems, files or applications, ensuring that the user receives the permissions associated with their role.

Entra ID, formerly known as *Azure AD*, is Microsoft's cloud-based IAM service. "It provides secure access to applications, devices, and data by verifying identities and enforcing access policies across hybrid and multi-cloud environments". (Jones 2025). For example, an Azure admin account can be created through the IAM system, and cloud-related membership groups can then be assigned to it.

The *business applications* shown in the graph may include for instance finance systems like ERP (Enterprise Resource Planning) systems or other core enterprise tools used in daily operations. These applications are considered as target systems, meaning they are the end destinations where user accounts, roles and access rights are provisioned by the IAM system.

Data is transferred between systems through *connectors*, as illustrated by the solid arrows in the figure 2. Connectors serve as integration interfaces that enable data flow in one or both directions. Connector can contain both collector and provisioner. The collector component retrieves, "reads", data from external systems into the IAM environment, while the provisioner component pushes, "writes", data from IAM to target systems. Info is stored in databases. Dashed arrows in the figure 2 represent authorisation processes. When a user signs in to a business application, the app sends an authorisation request to a system like Entra ID. Entra ID then verifies whether the user has the necessary role to access the application.

2.3 Security perspective

In the manufacturing industry, businesses are engaged in the production of physical goods, typically within highly automated environments. This process involves transforming raw materials into finished products using tools, machinery and human labour. Employees may work in underground facilities making tunnels and installing cables, or in other hazardous environments, when the IT systems must provide reliable access and functionality to support their daily tasks – weather they work in an office or inside a crane. Cybersecurity faces special challenges in these settings due to the presence of systems in production environments that may not be directly connected to the IAM system. As a result, manual input is often required, increasing the risk of human error (Chief Information Security Officer, interview 2025). In such environments, effective IAM plays a critical role in ensuring operational safety and continuity.

Without robust IAM practices, controlling access to critical systems becomes nearly impossible. IAM ensures that only authorised personnel can access and operate sensitive assets, while also enabling secure interactions between users and applications. Productivity is directly tied to access - if a worker cannot use the necessary systems, they are unable to perform their duties effectively. Similarly, if a security application fails to retrieve essential information, it can disrupt the entire production line, potentially costing thousands of euros per hour.

On the other hand, one of IAM's key responsibilities is to maintain appropriate and up-to-date access rights to prevent users from accumulating excessive privileges, particularly during role changes and offboarding. Delays or inaccuracies in updating permissions can create serious security risks. As the cybersecurity representative from the Company X notes, from a cybersecurity perspective, these transition points are critical for maintaining secure operations (Chief Information Security Officer, interview 2025). Another common issue is the complexity of IAM systems, which can make it challenging for users to select the correct roles from hundreds of options. As a result, users may request mirrored access based on another employee's profile, which can lead to excessive or inappropriate permissions.

Manufacturing companies operate under strict regulatory frameworks such as ISO standards, GDPR, and NIS2. IAM supports compliance by logging all identity-related actions - account creation, role changes, access approvals - providing a transparent and traceable audit trail of who did what, when and where. These are called as audit logs, serving as critical evidence for compliance and security reviews.

3 STAKEHOLDER IDENTIFICATION

The purpose of this thesis was to identify the key stakeholders interacting with IAM and to understand their needs and expectations. The expectation was that IT users were the intensive IAM users, but the aim was to broaden the view beyond them. In this section reviews all stakeholders interacting with IAM on some level and identifies the crucial groups for the study.

A *stakeholder* is an individual or group involved in a project, sharing responsibility for its execution and holding a vested interest in its success (Dictionary n.d.). Stakeholders may include for example employees, customers, investors, and community groups. They are typically classified as either primary or secondary stakeholders: primary stakeholders are directly affected by the project, while secondary stakeholders are indirectly involved, often through business relationships. Stakeholders can be internal, operating within the organisation and actively contributing to its processes, or external, engaging from outside the organisation. (Hendricks n.d.). In this research, identifying the primary internal stakeholders was particularly relevant.

3.1 Internal stakeholders

The key question guiding stakeholder identification was: “Who are the intensive IAM users?”. A report generated from the IAM production system revealed that 1.299 unique staff members had submitted requests through IAM since 2023. To focus on gaining insights from the most active users, those who had made fewer than 10 requests were excluded, resulting in a target group of 335 users for further analysis.

The dataset of this IAM report was largely well-structured from the start, but some manual adjustments were necessary to ensure accurate categorisation. All disabled user entries were removed, and the remaining users were organised to their designated stakeholder groups. The report identified four primary internal stakeholder groups: Operations, IT, Finance and HR. Defining the correct group for each user was not always straightforward, as some of them appeared to operate at the intersection of two departments. Anyhow, it was important to ensure a relatively balanced representation between IT and other groups, as the aim of this study was to gain insights beyond technically oriented users.

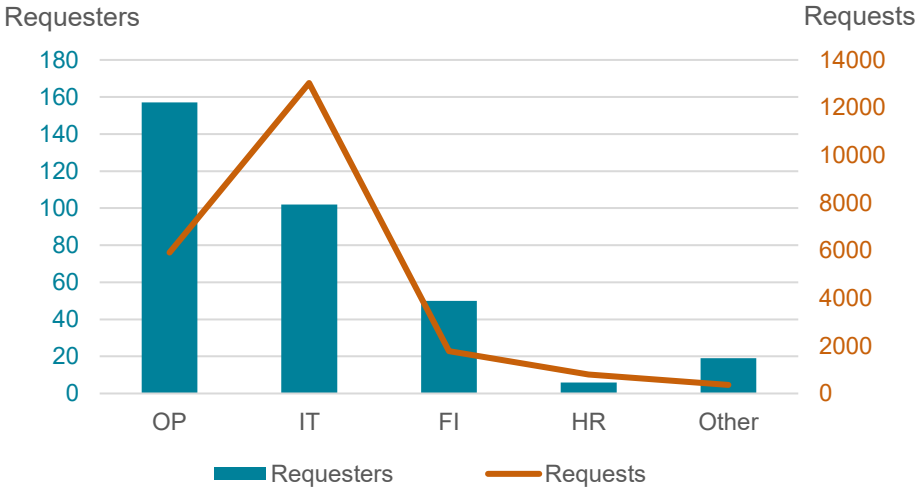

Figure 3. IAM usage volume by stakeholder groups

A common characteristic among the intensive requesters was that they often held managerial or team lead positions within their respective functions. The report revealed that the operations sector had the highest number of individual IAM users, as illustrated in the graph 3. In manufacturing business, operations cover the activities involved in converting the raw material into finished product. This group includes employees working in business support, process management and planning, technical implementation, logistics and automation. However, individual users in this group submitted relatively few IAM requests on average.

The second largest group by individual users was the IT sector. This group included ERP (Enterprise Resource Planning) system users, infrastructure specialists, IT architects, service owners, cybersecurity professionals, and IT support roles including IAM support. IT users accounted for the highest volume of IAM-related requests, which is visible as a peak in graph 3. This was expected, as they frequently interact with many digital systems.

The Finance stakeholders were the third biggest stakeholder group by the amount of active IAM users and completed requests. Finance department covers a wide range of sales functions including operational control, accounting, analytics and sales support. They help manage inventory, equipment, and staff costs to maintain operational stability and provide a clear picture of the company's financial situation, enabling leaders to make informed decisions.

HR personnel represented the smallest stakeholder group in terms of user count and executed requests in IAM system. Their responsibilities typically include managing the employee life cycle from recruiting, hiring, onboarding, and offboarding to processing payroll and leading HR-related projects and analyses. (Lucidchart n.d)

	Primary	Secondary
Internal	Operations IT Finance HR	Leadership Legal and compliance Blue-collar employees (e.g. Electrician)
External	IT service providers (e.g. Microsoft) Integration partners Identity verification services (e.g. BankID) Technical support partners	Customers Investors Vendors Regulatory authorities (GDBR2, NIS2, ISO)

Figure 4. Stakeholder quadrant

Beyond the primary internal stakeholders there are also other stakeholder groups that are affected by actions from IAM or contribute to IAM operations through indirect involvement. This study concentrated on the primary internal stakeholders but however, future research can benefit from identifying and including these additional stakeholders to gain a more comprehensive perspective. Stakeholder quadrant in the figure 4 illustrates both internal and external stakeholders, showing whether they are classified as primary or secondary.

Secondary internal stakeholders are indirectly impacted by IAM-related processes, often through primary internal users. This group includes teams within the organisation, such as senior leadership who make strategic decisions but may rely on support staff to handle IAM-related tasks on their behalf. Legal and compliance teams are also part of this group, as their responsibilities lie more on the regulatory side, as well as blue collar employees who focus on hands-on operational tasks.

3.2 External stakeholders

In addition to internal stakeholders, several external parties play a crucial role in supporting the IAM system, although they interact with it from outside the organisation and do not directly use it. These primary external stakeholders include IT service providers, integration partners, identity verification services, and technical support partners. They provide the infrastructure and support necessary for the IAM system but are not part of this research as they do not use the system themselves. IT service providers supply platforms such as Active Directory, Entra ID, and Microsoft Azure, which integrate with IAM workflows. Integration partners develop and maintain the connections between IAM and other enterprise systems. Identity verification services ensure secure onboarding and multi-factor authentication. Technical support partners, including IAM solution vendors, offer external assistance when needed.

Secondary external stakeholders include customers, investors, vendors, and regulatory authorities. Customers may be affected for example by the security measures enforced by IAM during their interactions with the organisation’s services, while investors are concerned with the IAM system’s ability to ensure business continuity. Regulatory authorities on the other hand impose requirements that the IAM system must meet to ensure compliance with legal frameworks, such as data protection laws and industry standards.

3.3 Importance of understanding the stakeholder view

Understanding the stakeholder perspective is essential for several reasons. First, recognising their roles and expectations allows for early identification of potential challenges, enabling proactive risk mitigation and more informed decision-making. Although IAM systems are often approached from a technical standpoint it is equally important to consider the needs of the user groups who interact with the system regularly. Stakeholder groups are not all the same and they may have different perspectives to convey, shaped by their work role or experiences. This may enhance the exchange of innovative ideas and lead to adaptive, sustainable solutions. (Kennedy 2025)

Secondly, incorporating stakeholder input enhances communication across teams and can positively influence the organisation as a whole. Engagement builds trust as stakeholders see that their opinions are valued and reflected in future actions. It may also reduce resistance to change when new systems are introduced.

4 RESEARCH IMPLEMENTATION

4.1 Goal of research and research questions

This thesis was conducted in cooperation with a global manufacturing organisation. The researcher works in the Company X within the End User Services team, which supports all the company's employees by ensuring that they have the necessary tools, such as workstations and software, and access rights to perform their work. Especially the work within the IAM team steered her interest toward IT security and data management. The commissioning company was also interested in gathering information about overall satisfaction with their current IAM system and whether the findings would indicate the need for its renewal. This led to the idea of conducting a stakeholder-driven analysis to better understand what different actors value in identity and access management and how those insights can inform system requirements in global manufacturing business.

The main research questions were:

1. Which stakeholder groups are interacting with the IAM system in the Company X?
2. What do these stakeholders need and value in an IAM system?
3. How current IAM solutions reflect the values and expectations identified in stakeholder survey and interviews?

4.2 Case study as a method

This research was conducted as a case study that combines both quantitative and qualitative data. Case study as a method offers an intensive understanding of a specific individual, group, organisation or process in a real-world context, whereas many other research methods are aiming to a wider generalisation. (Vuori 2021.) It is highly applicable for exploring human situations and identifying trends in opinions within a chosen area. Data is typically collected in narrative form, supported by observations, and later analysed under themes or ideas (Almeida, Andrade & Quintão 2020.)

To provide a versatile picture of the case, different source materials including questionnaires, interviews and system report were used in this thesis. The research target was an IAM system, and it was approached from the stakeholder point of view. Selected stakeholders were identified in the chapter 3 based on an IAM system report, which revealed the groups generating the highest number of requests within the system.

4.3 Collecting the research data via survey and interviews

Data for this research was collected through a structured survey created and distributed through Microsoft Forms platform. The survey was sent directly from the Forms portal to selected stakeholders who accessed it using their company email address. This also served to verify their identity, even though the data was analysed at the stakeholder group level rather than by individual responses.

Before sending the survey, a short cover letter was posted on the organisation's Teams channel to encourage users to take a moment for participation. They were informed that the company aimed to gather insights into stakeholder perspectives and values related to an IAM system, and that their input was highly valued. The survey itself included a brief description of its purpose to provide context for respondents.

The survey was open between 16.10-4.11.2025, giving participants 20 days to respond, and it was sent to 72 different stakeholders. Figure 5 shows that approximately half of the selected candidates were from the IT sector, as they were the most intense users of the IAM system. The other half came from Operations, Finance and HR. Stakeholders were selected based on the intensity of their IAM system usage: on average, IT users had submitted 240 requests per person during the past three years, and when IAM professionals were excluded, the average was 179. Operations users submitted an average of 131, Finance users 95 requests and HR users 25 per person.

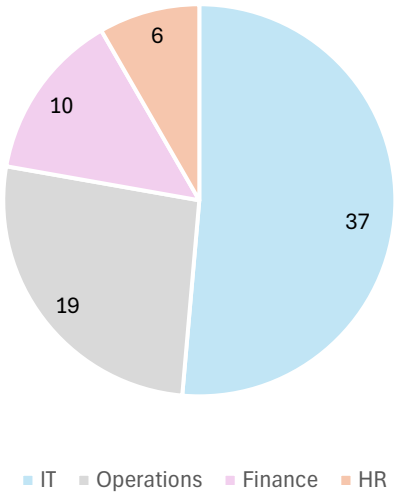

Figure 5. Survey distribution to 72 stakeholders

4.4 Data handling and analysis

Once the survey closed, it was time to start analysing the responses. The survey consisted of 15 questions, combining both quantitative and qualitative formats. Four questions used a Likert scale to measure opinions and attitudes across five levels of agreement, providing numerical data for analysis. Six questions were multiple-choice, allowing respondents to select from predefined options.

The remaining five questions were open-ended, giving participants the opportunity to express their thoughts in their own words. These responses were intended to elaborate on the Likert scale answers and predefined options, providing qualitative data that helped refine the numerical results. After collection, the answers were first cleaned of empty responses and then reviewed to identify whether they offered new perspectives beyond the stated standpoints. Most of the open-ended questions were optional and while the other questions were mandatory.

Also, three persons were interviewed to gain a deeper understanding of IAM practices and perspectives. One of the interviewees shared insights from the cybersecurity standpoint, complementing the theoretical discussion on IAM and security. The other two interviews focused on the user perspective: one approached IAM primarily from an internal controls' standpoint, while the other provided a technical expert view as an IAM consultant. Their insights are incorporated into the following results section to support the survey findings and provide additional detail.

5 RESULTS

Out of 72 stakeholders, 60 participated, resulting in a response rate of 83.3%. The questionnaire was divided into three sections. The first section covered background information about the respondents including which stakeholder group they represented, how frequently they used the IAM system, and how confident they felt using it. The second section explored their opinions on the current system: how they experienced its functionality and how well it served their needs. The final section focused on their values and expectations for an ideal IAM solution. Questions with the Likert scale were rated from one to five, one being the most negative value and five the most positive.

As seen in the figure 6, the largest stakeholder group was IT, representing 58% of respondents, while HR was the smallest at 5%. A few participants, originally categorised under the main four stakeholder groups, indicated belonging to other areas such as Strategy and Internal Controls. Because some stakeholder groups were very small, some containing only three representatives, it would have been challenging to obtain objective data from such small presentation. Therefore, the following charts present data in two categories: IT and Other, with the latter including all remaining stakeholders.

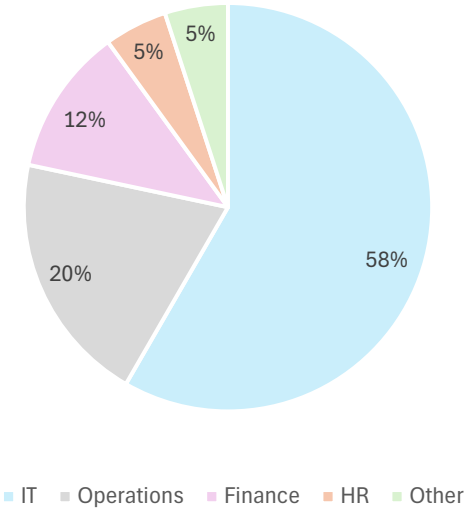

Figure 6. 60 survey participants by stakeholder groups

Stakeholder groups included individuals who used IAM system to varying degrees, depending on their role. The main user roles within the system are *users* who request access only for themselves, *managers* who can request access both for themselves and for their subordinates, *role approvers* who validate role-based requests such as membership applications, *role owners* who are responsible for managing specific roles and their configurations and *IAM support*, who provide technical assistance and maintain and develop the system. Additionally, IAM roles include an *Auditor* for reviewing audit logs to ensure compliance, risk mitigation and data protection. No auditors or users participated in this survey.

Most respondents operated within the IAM system in a manager role, as this was the selection by 80% of all respondents. Figure 7 shows that IT stakeholders were particularly concentrated in managerial positions, with some respondents coming from the IAM support. Roles in the Other group were more distributed, with higher shares of role owners and role approvers compared to IT. This suggests that IT's involvement in IAM is primarily administrative and technical, while other stakeholder groups are slightly more engaged in role ownership and approval processes

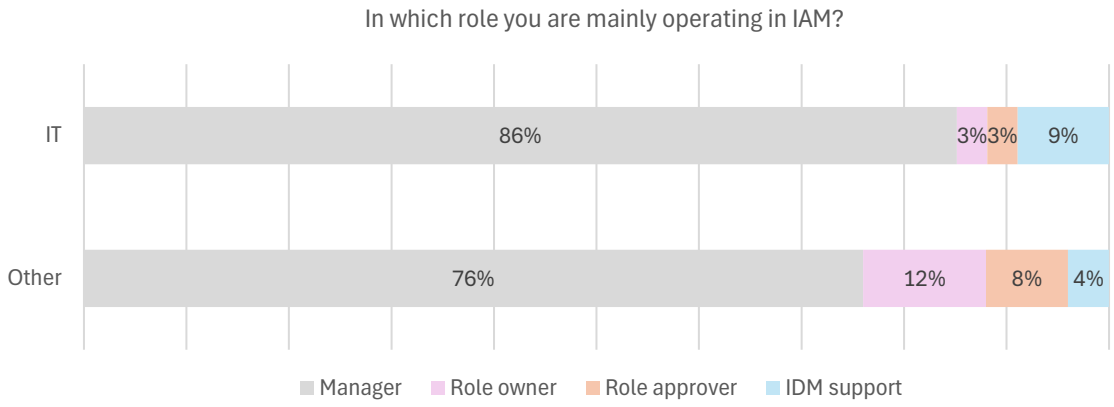

Figure 7. Roles when operating in IAM

Figure 8 presents the frequency of IAM use among respondents. Stakeholders interacted with the IAM system at varying levels. Maturity of IT stakeholders used the system weekly, whereas occasional use was more common among the Other group. 60% of all users used the system on daily or weekly bases suggesting that IAM is a regular tool in stakeholders' work.

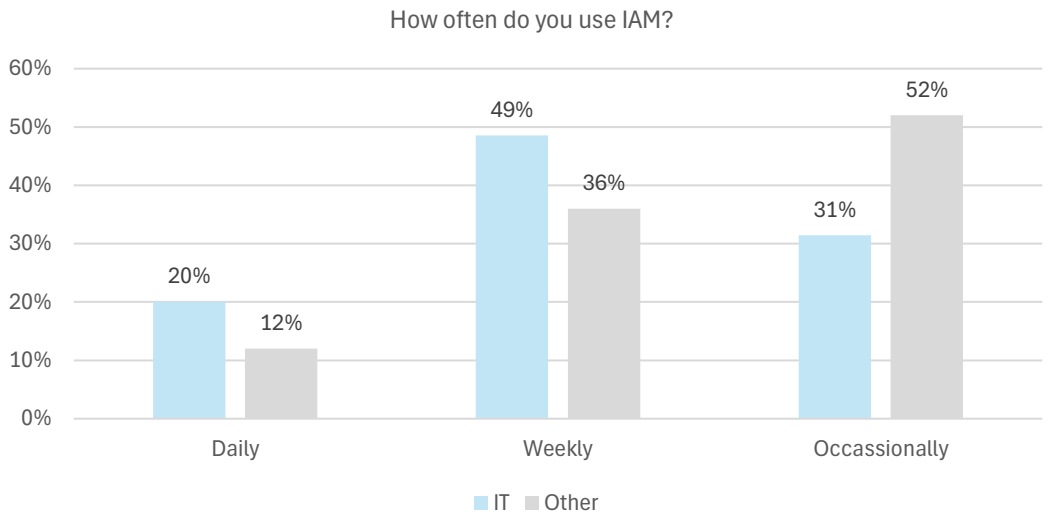

Figure 8. Frequency of IAM system use among respondents

Figure 9 presents most common tasks stakeholders perform in IAM system. Respondents could select one to three tasks from predefined options. As the most represented role was manager, also managerial actions were highlighted in the data.

IAM system is frequently used for creating external users, which accounts for 25% of responses, and updating their contract end dates, reported by 24% of respondents. When contracts are extended, managers must update this information in IAM to maintain access. Similarly, if a contract ends early, managers need to ensure access is revoked promptly.

Most common function among the external user creation was requesting new access, mentioned by 25% of respondents, either for a role or a license, which managers can request for themselves or to their subordinates. Internal employees are created in the HR system, and the initial accesses are granted as birthrights inside the IAM system. However, if more specific permissions are needed beyond standard access groups, they are requested separately. Responses also highlighted that IAM is used for approving or rejecting access requests, as managers often need to take these actions when requests are initiated by their subordinates.

Additionally, IAM serves as a source of user and access information, cited by 17% of respondents. Managers can view details of their own or their subordinates, while IT specialists can leverage this access for troubleshooting and assisting users. It is particularly useful for checking details such as user location, supervisor info or existing access rights.

IAM is also used for role creation, edition and deletion, though this was reported by only 6% of respondents. Users requesting these actions are often owners or approvers for multiple groups, which might explain why this option was less highlighted. Additionally, 4% of responses mentioned tasks outside predefined options, including IAM development activities by the IAM team and conducting access reviews from the role-approvers.

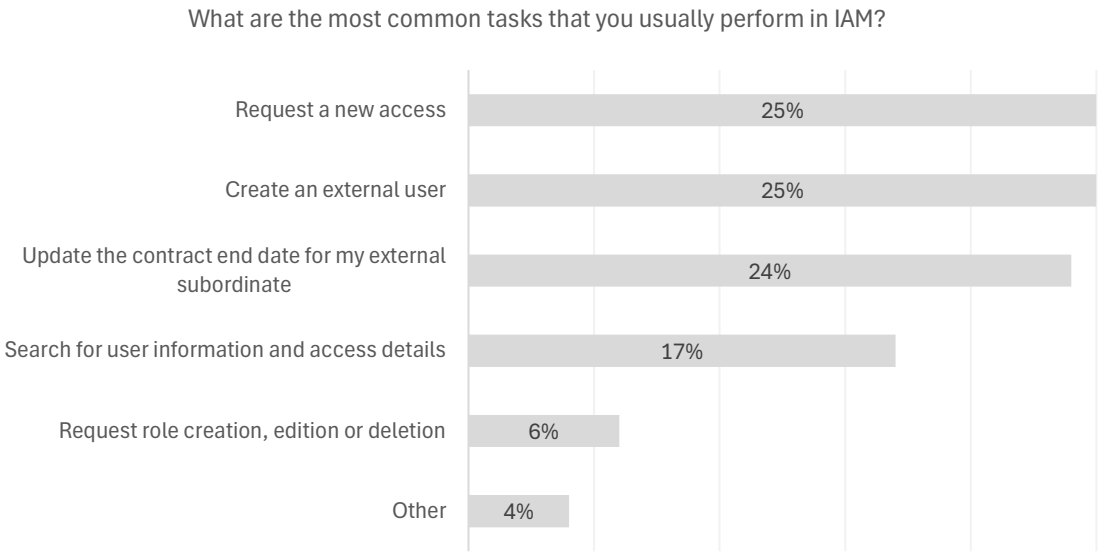

Figure 9. Most performed tasks

Figure 10 illustrates stakeholders' competence and capability when using the IAM system. As mentioned earlier, a total of 1.299 individuals had used the IAM system during the past three years, and 60 of the most intensive users responded to the survey. Therefore, these respondents had gained more experience with the system in comparison to an average user. Overall, most participants rated their confidence between "relatively confident" and "very confident."

IT stakeholders reported an average confidence level of 3.9, while other stakeholder groups averaged slightly lower at 3.6. Interestingly, IAM specialists had selected level 4, whereas many other users chose level 5. This may suggest that specialists, with their broader understanding of the system, recognise its extensive capabilities – some of which may not yet be fully utilised. Specialists commented that they feel confident using the system but noted that "workflow-related tasks require deeper understanding" and "there is still much to explore." Other users primarily used IAM for routine tasks they were comfortable with. As one respondent summarised: "I can perform any action I need in IDM," while another stated: "I know how to request externals because I have done it before. For a first timer, it could be difficult without help." When tasks fell outside routine processes, they were generally perceived challenging to implement, and extra support was needed.

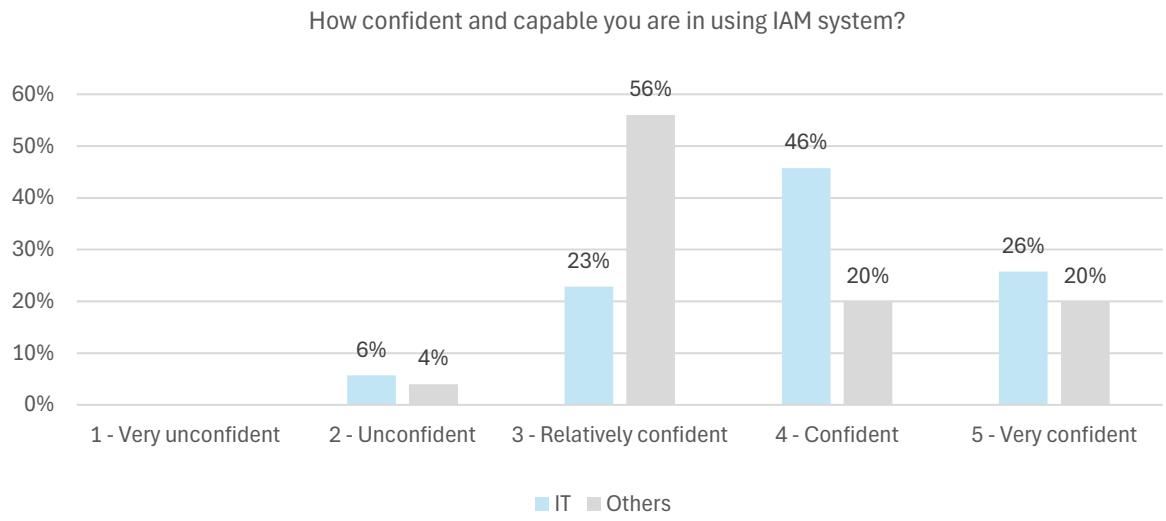

Figure 10. Confidence and competence in using IAM

5.1 Current situation and challenges

In the next part of the survey, the stakeholders rated their satisfaction both with the user experience and technical performance of the current IAM system. In general, respondents identified more room for improvement in the user interface than in the system's technical performance. As figure 11 shows, both IT users and Other stakeholders rated the user experience with an average of 2.9.

Open-ended explanatory questions revealed that stakeholders value clarity and intuitiveness in the IAM interface. Many expressed the need for easier navigation and a more logical structure, with one participant describing the current system "like walking in a strange town without a map." Ideally, the IAM system is so intuitive that users will not require a separate training to operate in it. Alternatively,

guidance could be integrated into the interface, or intelligent features such as AI-driven suggestions could assist users applying the correct roles.

When the system is unclear, it creates unnecessary administrative work and generates requests for the IAM team that should ideally be handled by end-users themselves. Respondents emphasised the importance of improving role search functionality, making frequently used actions more accessible, and providing an easily available action history.

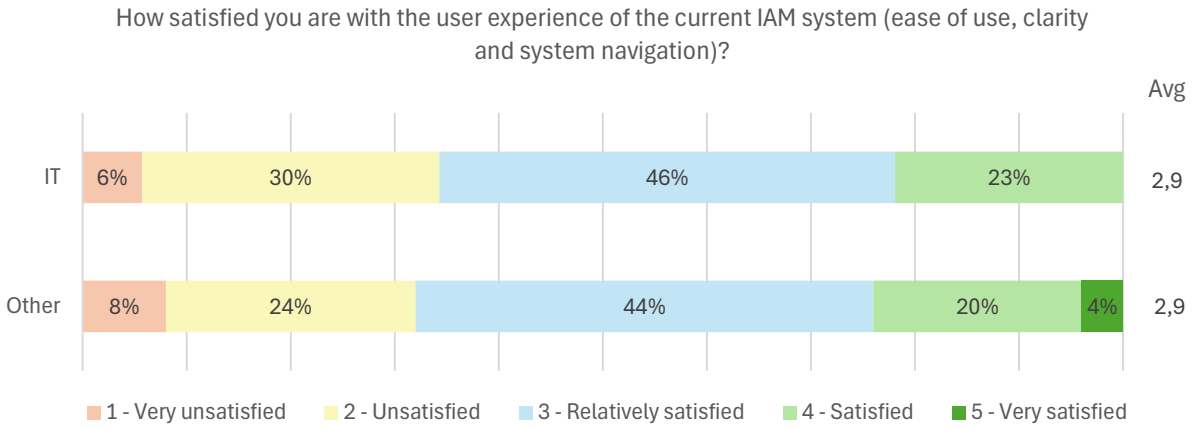

Figure 11. Satisfaction with the user experience

Figure 12 shows stakeholders' satisfaction with the technical performance of the current system. IT stakeholders rated it with an average of 3.1, showing a wide variation with responses, as the answers were ranging from very unsatisfied to very satisfied. Other stakeholders rated the system slightly higher, with an average of 3.5. This difference may reflect that IT users are more frequently exposed to system-level issues and troubleshooting tasks through various programs connected to IAM, which allows them to identify more areas for improvement. In contrast, users who are not involved in technical work typically notice problems only when the system fails.

Stakeholders emphasised that the technical performance of the IAM system should be reliable and free of frequent disruptions. Processes such as role approvals, external user creation and request handling should run smoothly without delays or stuck workflows in pending states. Users reported that these areas are not fully optimised and would benefit from improvements.

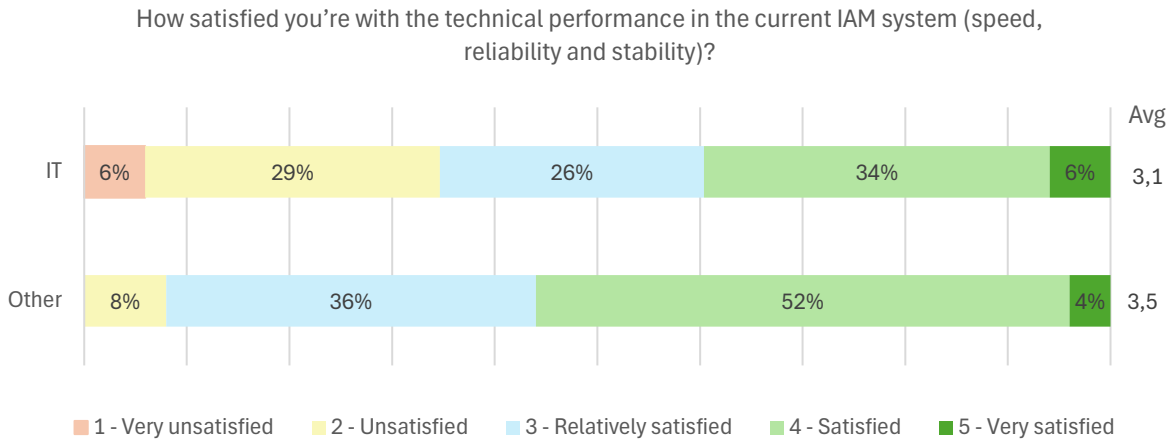

Figure 12. Satisfaction with the technical performance

At the end of the current state analysis, stakeholders were asked to identify the challenges they considered most significant. Respondents could select one to three options from predefined choices. As seen in the figure 13, the lack of clarity regarding which roles and permissions to request was rated as the most critical issue, cited by 29% of respondents. There are hundreds of applicable roles in the current system, making it difficult for users to determine what they actually need. This often leads to frustration and inefficiency when users do not know what roles to request, and IAM professionals must spend additional time clarifying the users' actual requirements to ensure that the principle of least privilege access is followed. Survey responses also emphasised the need to improve role descriptions to make selection easier.

Other significant challenge was the complexity of the user interface with 15 %, which was also emphasised in the interviews. Internal Controls representative in the Company X stated that users would benefit from a simplified initial view in the IAM portal, displaying default options for basic users (Head of Internal Control, interview 2025). Ideally, the interface could be pre-filtered and categorised based on logical criteria rather than displaying all options at once. The system could for example recognise the user's position and suggest relevant roles and permissions.

Three challenges were each reported by 13% of respondents: lack of guidance and support, tasks taking too long, and technical issues. These aspects reflect both interface complexity and system performance. When a system is not intuitive, additional training, support and documentation become necessary. At the same time, delays and errors highlight the need for better optimisation and reliability.

Stakeholders were given the opportunity to describe other challenges in an open-text field. These comments highlighted the need for automation, as many users felt that too much manual work was required, particularly for managers handling large numbers of external employees. They also stated that the missing entitlements were not monitored. Discussions with IAM professionals highlighted the need for system-level monitoring features that alert IAM administrators when processes fail, helping early detection of potential issues before they impact multiple processes.

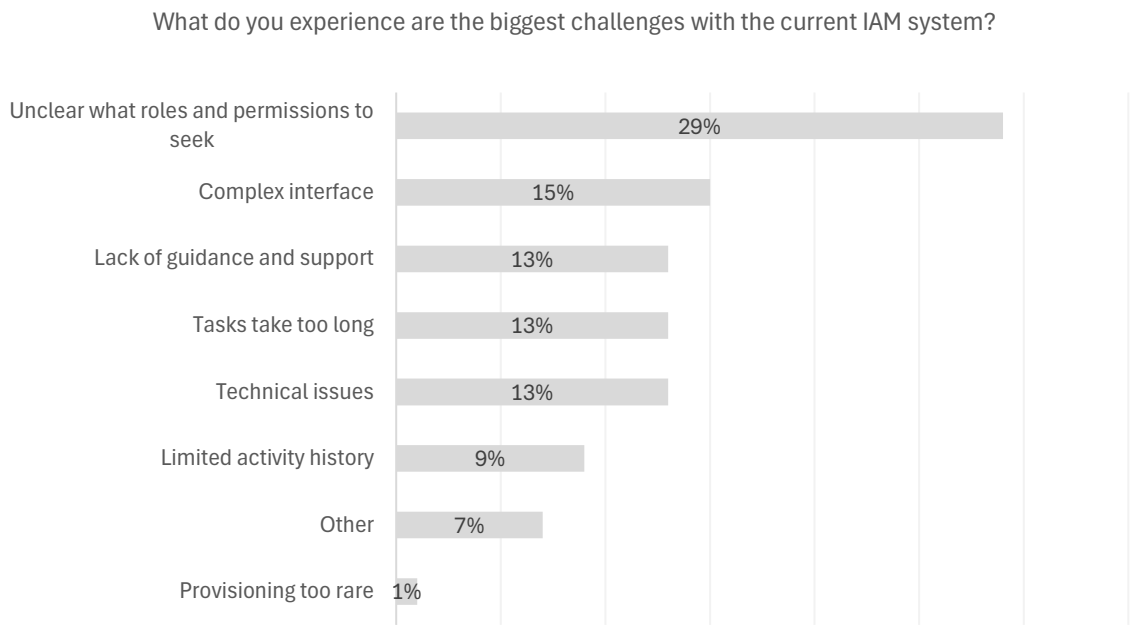

Figure 13. Biggest challenges

5.2 Values and expectations towards an IAM system

The previously mentioned challenges and the most important features highlighted similar aspects. Figure 14 presents an overall view of the results, while Figure 15 provides a more detailed breakdown by the two stakeholder groups. Stakeholders were asked to rate each predefined option on a scale from one to five, with five indicating ‘very important.’

Survey responses show that all mentioned features were considered important, as the maturity of the claims scored a rating of 4 or higher. Usability emerged as the most critical factor across all stakeholder groups. ‘Easy and intuitive user experience’ was clearly rated the highest, with an average score of 4.5. Anyhow, the visually appealing user interface wasn’t considered particularly important with the score of 3.2. Speed was also considered essential, scoring 4.4, as access rights should be granted or revoked quickly with as little friction as possible, and support should be available when needed. Architecture-related aspects were also emphasised, as stakeholders expected the system to integrate seamlessly with other organisational systems, scoring 4.2, and to maintain high fault tolerance and overall reliability, averaging 4.1.

Security ranked as another key area, scoring 4.4 alongside with fast and reliable access provisioning. One of the open-text responses brought up the principles of confidentiality, integrity and availability. Confidentiality ensures secure access management and provides a complete audit trail of who has access and why in the IAM system. Integrity refers to a fact that data is accurate, complete and unaltered, and that it remains trustworthy over its life cycle. Availability is also important aspect as the system is expected to be functioning without downtime or lengthy upgrades.

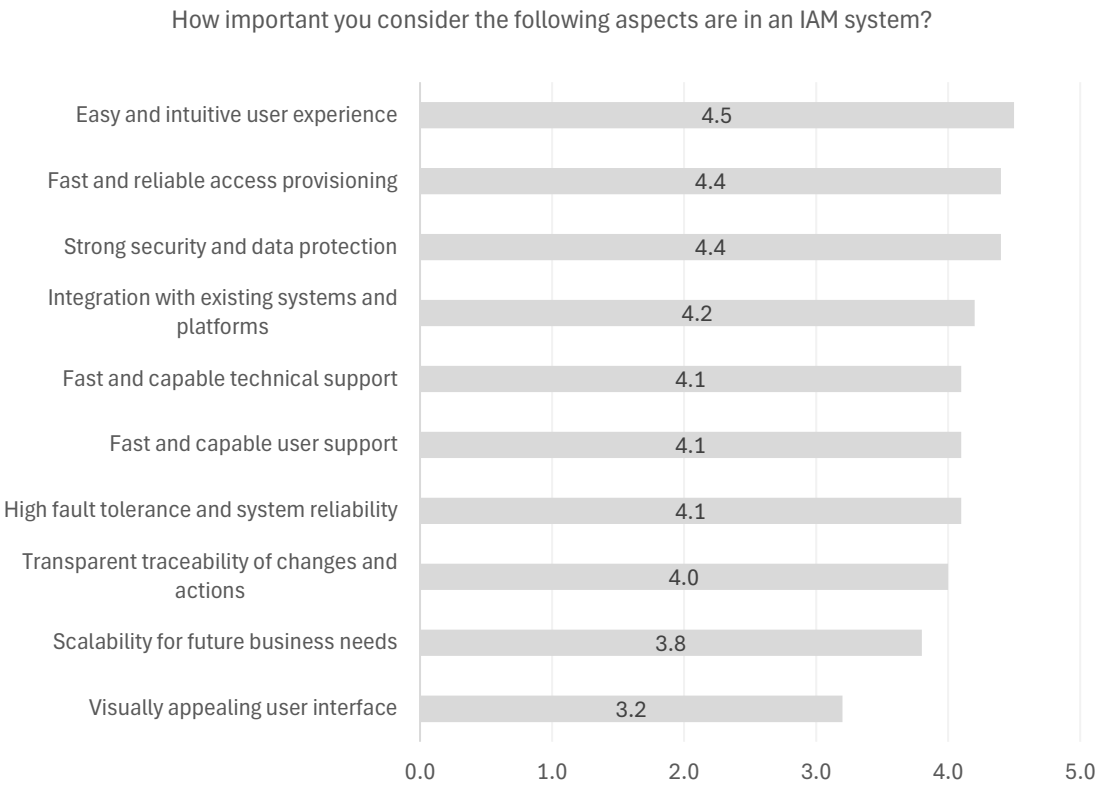

Figure 14. Important aspects

IT and other stakeholders shared a largely unified view, as most average scores differed by only 0.1 or 0.2 points. The biggest gap appeared in fast and capable user support, where the Other group rated it 0.5 points higher. IT users on the other hand placed greater emphasis on integration with existing systems and platforms, scoring it 0.4 points higher than the Other group.

Values	Usablity		Speed			Architecture			Security	
	Easy and intuitive user experience	Visually appealing user interface	Fast and reliable access provisioning	Fast and capable technical support	Fast and capable user support	High fault tolerance and system reliability	Integration with existing systems and platforms	Scalability for future business needs	Strong security and data protection	Transparent traceability of changes and actions
IT	4,5	3,1	4,5	4,0	3,9	4,3	4,4	3,8	4,5	4,1
Other	4,4	3,2	4,4	4,2	4,3	3,8	4,0	3,6	4,3	3,9
All	4,5	3,2	4,4	4,1	4,1	4,1	4,2	3,8	4,4	4,1

Figure 15. Important aspects considered by stakeholder groups

Finally, stakeholders were asked to summarise the benefits they expected most from the future IAM system. This question included slightly different predefined options. As automation was mentioned in several open-ended answers by the respondents, it became the most anticipated benefit when offered as a choice, cited by 22% of respondents. In connection to this, users also expressed interest in more self-service capabilities with 12%. As the Internal Controls representative in the Company X

suggests, for instance good reporting capabilities in IAM can enable authorised users to generate reports independently without contacting the IAM team (Head of Internal Control, interview 2025).

The second most desired improvement was better visibility for roles, permissions and access history, highlighted by 16 percent of respondents. As stated earlier, users appreciated the ease of finding required roles and the ability to track the status of their own requests. In terms of reporting, one respondent noted it would be useful to generate reports of their subordinates for example by filtering employees based on specific authorisations e.g. “maintenance planner”.

Seamless integration with other systems was close behind at 15 percent, followed by faster access management at 14 percent. Interestingly, an improved user interface ranked only fifth among eight different benefits, with 13 percent mentioning it. Presumably, clearer role and permission visibility would also contribute to a better UI, so these features are closely linked. Respondents did not see a strong need for improved security, which was cited by only 5 percent, and fault tolerance was the least mentioned benefit at 3 percent, indicating general satisfaction with the current state.

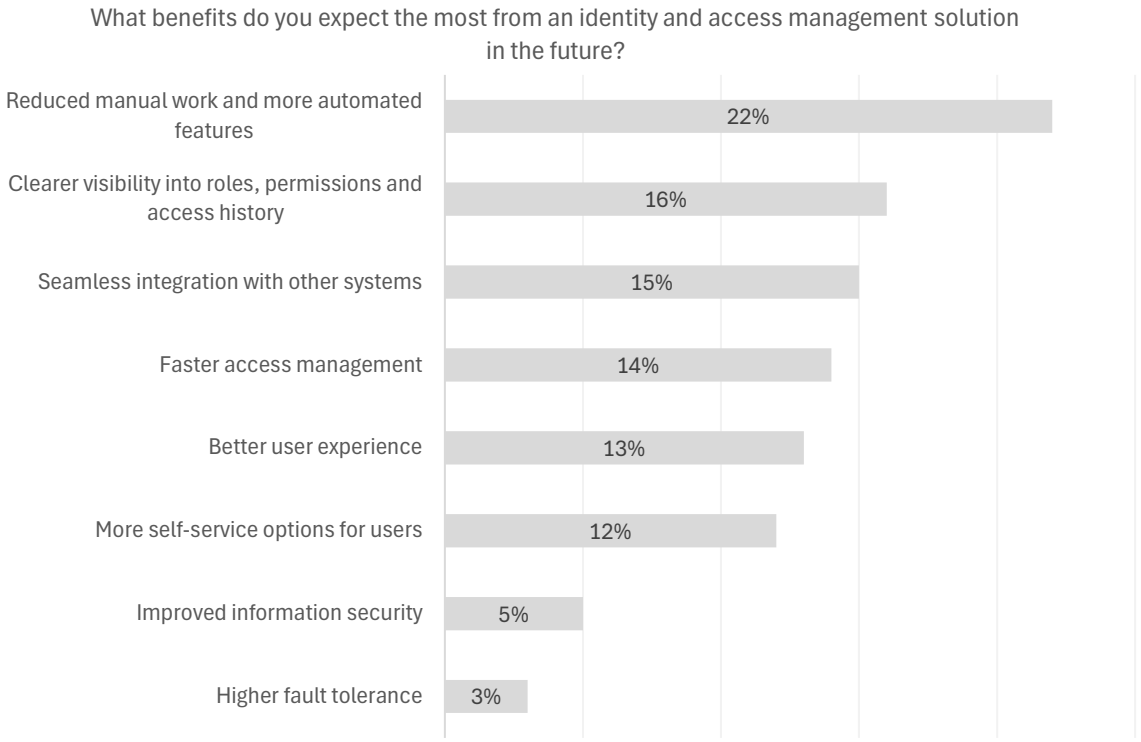

Figure 16. Expected benefits from the IAM system

6 REFLECTING STAKEHOLDER EXPECTATIONS IN CURRENT IAM SOLUTIONS

6.1 Mapping results to selected solutions

According to the survey, most of intensive users worked in managerial roles, with some overseeing dozens of subordinates. They appreciate a clear and intuitive user interface, automated features, and expanded self-service options in an IAM system. Respondents also emphasised the need for a clear visibility of requestable roles and permissions, as well as improved monitoring capabilities for IAM administrators.

Seamless integration with other business processes was also highlighted in the survey answers. Modern IAM solutions are typically modular, meaning that the system is divided into smaller, independent components. This reduces complexity and makes the software easier to manage and update as changes can be targeted to a single module without affecting the entire system (Owox n.d). As Kotilainen (2025) mentions, modularity increases flexibility and allows the system to adapt to different integration methods and workflows. Respondents in IAM support roles emphasised the benefit of having a native integration to critical systems such as ERP and supporting systems like the ticketing platforms. In contrast, if an IAM system requires extensive customisation to create these integrations, it can result in a fragmented and complex architecture that depends heavily on detailed documentation (Kotilainen 2025).

Some survey responses suggested leveraging artificial intelligence to recommend roles and other access based on a user's work role. Gartner studies encourage companies to prioritise intelligence when selecting IGA technologies, as these solutions are evolving rapidly and significantly improve efficiency. Besides providing access suggestions, AI can be applied in analytics for example to identify users with excessive privileges and thereby support security risk management. This makes troubleshooting faster and reduces manual work. However, adopting AI in IAM systems remains challenging due to issues such as insufficient or poor-quality in the organisational data and concerns about using AI for high-risk access decisions. (Archambault, Harris & Mezzera 2024,25.)

The final research question was to review how current IAM solutions reflect the values and expectations identified in stakeholder survey and interviews. Gartner studies remind that when selecting an IGA solution, organisations should consider both short-term requirements and long-term strategic needs, because full implementations, including integrations with target systems, can take years. There are at least 55 different solutions on the market, each offering varying features. (Archambault etc. 2024, 13 & 25). For this review, three IAM solutions were selected for deeper analysis based on their distinct approaches: RSA as an on-premises system, SailPoint offering a cloud-based solution Identity Security Cloud with AI capabilities, and Clear Skye running natively on ServiceNow ticketing platform.

6.1.1 RSA IG&L

RSA Identity Governance and Lifecycle is an identity and access management solution originally developed by Aveksa Inc, founded in 2004 in Waltham, United States. Aveksa was acquired by RSA Security in 2013, after which the product became part of the RSA IAM portfolio (Tracxn, 2025).

RSA IG&L is known as on-premises solution that has been on the market for over 20 years serving many large and complex environments (Data, Guthrie, Harris, & Murphy 2024, 15). It has long been

a strong choice for businesses, consistently performing well in Gartner's IAM solution comparisons. Nowadays, RSA also has also a Saas solution available (RSA n.d).

The RSA user interface is rather traditional, requiring training before it can be used effectively. System includes basic monitoring and reporting features, such as identifying failing connector collections, but it does not actively alert IAM administrators. Many processes in the RSA solution are automated, and there are many functionalities to be leveraged (Kotilainen 2025). The newest release, version 8, is advertised to have Advanced Dashboards which enhances monitoring by unifying fractioned data into intuitive visualisations (RSA n.d). RSA modularity is on moderate level, and its documentation does not directly mention supporting AI capabilities.

6.1.2 Clear Skye

Clear Skye is a cloud-based identity governance management software provider, founded in Emeryville, United States (Tracxn, 2025). It is integrated into the ServiceNow ticketing system, allowing users to request access directly within the platform, which makes the process fast and simple for both end users and IAM professionals. If the company is already using ServiceNow, the user interface may feel familiar and easy to use. Users do not need to learn a new system, as they can request access through the same interface they use to order a laptop, for example. The system style aligns with ServiceNow's design across different views and forms. (Clear Skye 2022)

Clear Skye is a modular system with a wide selection of connectors for integrating with numerous applications. In terms of monitoring, the system connects to the Integrated Risk Management (IRM) tool, which enables automated tracking of compliance and risk. (Clear Skye n.d) Artificial intelligence capabilities are being introduced to Clear Skye as part of their AI strategy, which focuses on improving visibility into user access and enhancing observability to identify potential risks (Teacher 2025).

6.1.3 SailPoint

SailPoint was founded in 2005 in Texas, United States, and offers two Identity Governance and Administration (IGA) solutions: the on-premises platform IdentityIQ and the cloud-based SaaS solution Identity Security Cloud. (Data etc. 2024, 22) Both solutions provide advanced analytics and automation capabilities, and they are designed as modular systems.

SailPoint Identity Security Cloud is known for its user-friendly interface, which is intuitive to use and simple to navigate. System has high-level automation and a wide range of pre-built connectors making it flexible across diverse environments (Peerspot n.d.). Sailpoint's AI journey began already in 2017, and today Identity Security Cloud offers an AI tool with machine learning capabilities to help mitigate potential security risks, such as detecting unusual user behaviour (Canvas Business Model 2025; Erkenborn & Wikström 2025).

Based on the SailPoint documentation, the system reporting is comprehensive, as nearly every activity within the system is captured in audit reports. Additionally, it is possible to configure Identity Security Cloud to send notifications when certain components on the site have problems. (Sailpoint Identity Services n.d.) However, according to some reviews, the platform is technically complex to configure, which may require significant expertise for a full deployment (Brooks 2024).

6.1.4 Summary of solutions

Figure 17 presents a table comparing the three solutions and their key capabilities. As mentioned earlier, there are many more IAM solutions on the market, and organisations should prioritise their criteria based on their specific needs. Finding a single solution that meets all requirements can be challenging; however, many options are flexible, and additional integrations can often be added later to extend functionality. It is good to note that skilful and well-planned customisation plays a crucial role in enhancing usability whereas poorly implemented modifications can make an otherwise good system complicated and difficult to maintain.

One aspect not covered in this review is cost, which includes both the initial deployment expenses, annual licensing fees and continuous service support. Licensing model can be based on the company size or the amount of IAM users for example. Version updates and new integrations require service support which may also create additional expenses. These factors naturally play a significant role in shaping the final decision.

Solution	Clear UI	Monitoring and reporting quality	AI capabilities	Native ticketing integration	Modular architecture	Deployment model
RSA IG&L	Moderate	Moderate	No information	No	Moderate	On-Premises and cloud
Clear Skye	Good	Good	Upcoming	Yes	High	Cloud
SailPoint Identity Security Cloud	Good	High	Yes	No	High	Cloud

Figure 17. Comparison of IAM solutions

7 DISCUSSION

7.1 Review of research results

I began exploring the world of IAM in summer 2025 and gradually developed an understanding of different IAM processes through the work at Company X. This provided the foundation for the thesis theory section, which I aimed to make accessible for readers unfamiliar with IAM, and avoid unnecessary detail since IAM is a broad field despite its relatively short history. Additionally, several graphs were included to highlight the key findings and to improve clarity, making results easy to interpret in visual form. The research itself was conducted alongside my regular work during the autumn semester of 2025. The survey response rate was 83.3%, which is a good number and suggests that the answers reflect the values and expectations of IAM stakeholders in the company.

The first goal of this thesis was to identify the key stakeholders who use the IAM system most frequently in the Company X. The results show that the most intensive users typically hold managerial positions in IT, Operations, Finance, and HR, with 60% of them using the system on a daily or weekly basis. This highlights IAM's strategic importance and its role as a regular tool in stakeholders' work. IT had the highest concentration of intensive users, whereas Operations had the broadest user base with many occasional users, suggesting that the system is serving a wide range of users. Although the categorisation by departments is broad, it served the purpose of this research. Since IT was clearly the most represented group in the survey responses, and other stakeholder groups had only a few respondents, presenting the survey findings in two categories, IT and Other, was a logical choice.

The second objective was to explore what stakeholders need and value in an IAM system. Respondents shared their views through a survey, and some were also interviewed. Across stakeholder groups, the responses were largely consistent. They place the highest value on a clear and intuitive user experience, fast and reliable access provisioning, and strong security and data protection. When asked about the most anticipated benefits of a future solution, based on a slightly different set of options, they selected automation, improved visibility of roles, and seamless integration. In addition, IAM experts emphasised that the system should be modular to meet modern standards, support critical organisational systems such as ERP, and potentially enable ticketing integrations and leverage AI.

The final research question explored how current IAM solutions reflect the values and expectations identified in the stakeholder survey and interviews. Three products were compared: RSA, Clear Skye, and SailPoint. These were selected because they represent very different approaches: one known as an on-premises system, one integrating with cloud and ticketing platforms, and one being a cloud-based solution with strong AI capabilities. However, gaining a comprehensive understanding of these systems proved challenging, as interface images and functionality demos were often unavailable online. This highlights the importance of requesting live vendor demonstrations and possibly conducting pilot testing in trial environments before making a purchase decision. Nevertheless, the comparison revealed that a single solution meets seldom all requirements and customisation in some level is often needed. With many IAM solutions available on the market, organisations need to prioritise the features that matter most.

7.2 Ethics and reliability of the research

Measuring the reliability and validity of a case study can sometimes be challenging. Responses may not be objective, or the researcher may anticipate a specific outcome. Survey questions can leave out important areas or highlight the others. That is why the work plan is essential, clarifying what are the goals and how they will be approached.

In this research, I have aimed to describe the research process and the participating stakeholders in detail to give the reader a clear understanding of what this thesis examines. The Teams cover letter a bit before the survey distribution provided participants with an advance overview of the study and its objectives, and the survey introduction repeated the purpose of the research. The survey itself (Attachment 1) was designed to be as clear as possible, and to cover the main researchable areas.

Reliability of the research refers to consistency: if the research was repeated, would it lead to the same results? Validity on the other hand concerns whether the study measures what it was intended to measure. (Bets 2025) Case studies often rely on relatively small samples (Almeida e.g. 2020), and in this research, 60 stakeholders shared their views. This research focused on a large enterprise operating in the manufacturing sector, but its findings cannot be generalised to other manufacturing businesses without conducting similar surveys elsewhere. However, these results provide useful info about the stakeholders involved in an IAM system within the Company X, as well as their expectations for such a system.

One way to test the reliability and usability of this study would be to repeat the survey with a set of intensive IAM users in another manufacturing business, and see what results they get regarding the satisfaction with their current system and the values and expectations associated with IAM. In this research, three participants were interviewed, but involving more stakeholders from different fields in the interviews could help validate the findings. A larger sample and multiple iterations strengthen the reliability assessment and provide deeper insights into whether the results remain consistent over time. It is also important to note that as technology and business environments evolve rapidly, user expectations will change as well. Therefore, future surveys should be adapted accordingly to reflect these shifts.

Case study is primarily a qualitative method, but it can also contain quantitative elements, as was done in this thesis. This combination made it possible to present data numerically and put different IAM system requirements and claims in an order according to the responses. Case studies are particularly useful when the researcher has limited control over the phenomenon being examined, such as opinions or expectations. Case study helps to understand the context and the reasons behind certain opinions (Almeida et al., 2020). User experiences are personal and depend on the user's familiarity with the system and prior experience, therefore case study was a good method for this research. It was also important to include interviews and open-ended questions, allowing participants to share insights that might otherwise remained unspoken.

When conducting research, it is essential to follow ethical principles to protect participants and maintain the integrity of the study. Participant data must be in safe through restricted access, and participation should always be voluntary. Ethical practices also enhance objectivity and accountability, helping ensure that research findings are accurate and applicable (Omnistar, 2025). In this study, users completed the survey via Windows Forms, which validated their identity through a company

email. Interviews were conducted using Microsoft Teams, ensuring data security while providing a convenient way for participants to join. Survey responses remained anonymous, as participants were represented only by their stakeholder groups. Interviewees were also anonymised, but their job titles remained visible to provide context about their perspective.

7.3 Suggestions for further research and the significance of the thesis

Future research could take a broader stakeholder perspective. Secondary internal stakeholders, such as blue-collar workers who only request roles for themselves, could be included, as these stakeholders were completely excluded from this study. Including these users might provide valuable insights into the usability and intuitiveness of the user interfaces, since they interact with the system infrequently and could offer fresh perspectives. In addition, exploring external stakeholders could bring meaningful insight, for example, understanding which aspects integration partners would prioritise in IAM solutions.

Stakeholders could also be categorised in greater detail for instance by specific job roles. Previous studies have identified groups such as IT Infrastructure, Network Management, Support, Platform Owners, Help Desk, Strategy, and Business Units. Tailoring survey questions for these groups could help capture role-specific needs and challenges more effectively. However, one of the initial aims of this thesis was to look beyond the IT perspective by including other stakeholders, such as HR, Finance, and Operations, in the conversation and explore also their needs. This goal was successfully achieved through the study.

This study serves as an initial investigation by identifying key expectations and needs across departments. Future research could take a more detailed and technical approach for example by exploring which specific tasks stakeholders would like to automate, as automation was mentioned as a desired feature. It would also be valuable to understand what stakeholders consider clear and intuitive in a user interface, since the challenge lies in defining and quantifying what a good user experience means for an IAM solution in practice. Gathering feedback from users with prior experience in other IAM systems could provide particularly useful insights.

This thesis holds both practical and strategic value for the commissioning organisation. Rather than focusing solely on technical comparisons, it has uncovered what different user groups value in IAM systems within a global manufacturing context. These insights form a foundation for defining system requirements that reflect real operational demands. Furthermore, involving stakeholders in this process ensures their voices are heard, fosters collaboration, and strengthens the sense of shared responsibility within the organisation. This study offers an overarching view of values and expectations, creating a basis for the future work to go deeper into technical details and specific implementation aspects.

For the researcher, the thesis offered an opportunity to deepen the expertise in IAM, while also strengthening the skills in information retrieval and communication with both technical and business stakeholders. Planning and conducting interviews thought a lot about gathering insights and analysing it. One finding was that the quality of the survey questions influences the answers received – well-defined questions lead to precise information, whereas vague questions result in generic responses. Carefully designed survey ensures that all important aspects are covered, as some details may remain hidden unless they are directly asked. Collecting information from vendor websites was

sometimes challenging, as many details were not stated explicitly and required interpretation. It became clear that live vendor presentations are crucial when gathering well-structured overview of the solution. Through this study, researcher also became more familiar with colleagues across departments and gained an understanding of how large projects are approached in a global organisation.

REFERENCES

Artificial intelligence has been used in the work as follows:

Microsoft Copilot. (2025). Conversational AI assistant powered by GPT-4. Microsoft. Utilised to help the researcher understand different aspects related to IAM, and to correct grammar. December 2025. https://www.microsoft.com/copilot.

Microsoft Copilot for Microsoft 365. (2025). Conversational AI assistant powered by GPT-4. Utilised to make interview memos. November 2025. https://www.microsoft.com/microsoft-365/copilot

Almeida, F., Andrade, P. & Quintão, C. 2020. How to Improve the Validity and Reliability of a Case Study Approach. https://files.eric.ed.gov/fulltext/EJ1294617.pdf. Journal of Interdisciplinary Studies in Education. 9(2), 264–275. Referenced 19.11.2025.

Archambault, R., Harris, N. & Mezzera, P. 2024. Gartner: Market Guide for Identity Governance and Administration. Reports and studies. Referenced 15.11.2025.

Awati, R., Chai, W. & Gillis, A.S. 2025. What is Active Directory (AD)?. TechTarget blog. Published 11.4.2025. https://www.techtarget.com/searchwindowsserver/definition/Active-Directory. Referenced 21.9.2025.

Bets, A. 2025. Reliability vs Validity in Research. Online source. Published 10.11.2025. https://www.researchprospect.com/reliability-and-validity/. Referenced 20.11.2025.

Brooks, F. 2024. SailPoint Identity Security Cloud: An Honest Review | Pros and Cons. Video. YouTube video service. Published 7.12.2025. https://www.youtube.com/watch?v=U79BBRpdChA. Referenced 16.11.2025.

Chief Information Security Officer 2025. Company X. Interview 11.11.2025.

Canvas Business Model 2025. What is the brief history of SailPoint company? Online Source. Published 12.7.2025. https://canvasbusinessmodel.com/blogs/brief-history/sailpoint-brief-history#:~:text=SailPoint%27s%20journey%20began%20in%202005%20in%20Austin%2C%20Texas%2C,need%20for%20robust%20identity%20and%20access%20management%20solutions. Referenced. 16.11.2025.

Clear Skye 2022. Clear Skye IGA: Self-Service Access. Video. YouTube video service. Published 26.1.2022. https://www.youtube.com/watch?v=2yfTXivScoI. Referenced 16.11.2025.

Clear Skye n.d. Simplify Access Reviews while enhancing security and regulatory compliance. Online source. https://clearskye.com/products/capabilities/access-review. Referenced 1.12.2025.

Cloudworks n.d. Mitä identiteetin- ja pääsynhallinta (IAM) tarkalleen ottaen on? Online source. https://www.cloudworks.fi/artikkelit/mita-on-identiteetinhallinta#:~:text=IAM%2C%20eli%20Identity%20and%20Access%20Management%2C%20tarkoittaa%20identiteetin-,%E2%80%93%20ei%20enemp%C3%A4%C3%A4%20eik%C3%A4%20v%C3%A4hemp%C3%A4%C3%A4.%20Mit%C3%A4%20on%20identiteetinhallinta%3F. Referenced 29.8.2025.

Data, A., Harris, N., Guthrie, B. & Murphy, J. 2024. Gartner: Magic Quadrant for Access Management. Reports and studies. Referenced 16.11.2025.

Erkenborn, S. & Wikström, M. 2025. SailPoint Identity Governance presentation 10.12.2025. Sailpoint.

Fortra 2020. What’s the Difference Between IAM, IGA, and PAM? Online source. Published 24.7.2020. https://www.coresecurity.com/blog/whats-difference-between-iam-iga-and-pam. Referenced 20.9.2025.

Head of Internal Control 2025. Company X. Interview 13.11.2025.

Hendricks, A. n.d. Types of Stakeholders and Their Roles: A Quick Reference Guide. Simply stakeholders' blog. https://simplystakeholders.com/types-of-stakeholders-and-their-roles/. Referenced 24.9.2025.

Jones, R. 2025. Microsoft Entra ID Explained: What It Is, How It Works & Why It Matters in 2025. Online source. Published 7.11.2025. https://www.netcomlearning.com/blog/microsoft-entra-id-all-inclusive-guide. Referenced 21.9.2025.

Kennedy, E. 2025. Why is effective stakeholder engagement important? Online source. Updated 18.9.2025. https://blog.jambo.cloud/10-reasons-why-effective-stakeholder-engagement-is-crucial. Referenced 27.11.2025.

Kotilainen, J. 2025. IAM Consultant. IQI Success Insuring Oy. Interview 15.11.2025.

Lucidchart n.d. What does HR actually do? 11 key responsibilities. Online source. https://www.lucidchart.com/blog/what-does-hr-do. Referenced 14.11.2025.

Meile, F. 2024. The evolution of Identity Management: A timeline of growth and importance. Online source. Published 29.10.2025. https://www.skypro.eu/the-evolution-of-identity-management/. Referenced 30.8.2025.

Microsoft n.d. What is identity and access management (IAM)? Online source. https://www.microsoft.com/en-us/security/business/security-101/what-is-identity-access-management-iam?msockid=2e797b9637f26cb715696df536da6d45. Referenced 21.9.2025.

Microsoft Ignite 2025. Identity and access management fundamental concepts. Online source. Updated 21.8.2025. https://learn.microsoft.com/en-us/entra/fundamentals/identity-fundamental-concepts. Referenced 30.9.2025.

Owox n.d. What Is Modularity? Online source. https://www.owox.com/glossary/modularity. Referenced 15.11.2025.

Omnistar 2025. What is Ethics in Research? Key Principles, Challenges & Best Practices. Online source. Published 25.8.2025. https://www.omnistar.cloud/insights/what-is-ethics-in-research/. Referenced 14.11.2025.

PeerSpot n.d. SailPoint Identity Security Cloud Reviews. Online Source. https://www.peerspot.com/products/sailpoint-identity-security-cloud-reviews. Referenced 29.11.2025.

RSA n.d. RSA Governance & Lifecycle Advanced Dashboards. Online shource. https://www.rsa.com/resources/solution-briefs/rsa-governance-lifecycle-advanced-dashboards/. Referenced 30.11.2025.

RSA n.d. RSA Governance & Lifecycle - Comprehensive identity governance & administration (IGA) on-premises and in the cloud. Online source. https://www.rsa.com/resources/datasheets/rsa-governance-and-lifecycle/?utm_source=chatgpt.com. Referenced 30.11.2025.

Sailpoint Identity Services n.d. Audit reports and Monitoring. Online source. https://documentation.sailpoint.com/saas/help/common/audit-reports.html. Referenced 1.12.2025.

ServiceNow Store n.d. Online source. Clear Skye Inc. https://store.servicenow.com/store/seller/2754ec66db5c2a84f9f77c541f961950#:~:text=Clear%20Skye%20delivers%20a%20complete%20Identity%20and%20Access,automation%2C%20access%20requests%2C%20access%20certifications%20and%20business%20intelligence. Referenced 21.11.2025.

Teacher, B. 2025. Clear Skye Phase 1 AI: Bringing Visibility and Observability to Identity. Online source. Published 15.9.2025. https://clearskye.com/blog/clear-skye-phase-1-ai-bringing-visibility-and-observability-to-identity. Referenced 1.12.2025.

Tenable 2025. Key components of identity and access management (IAM). Online source. Updated 18.8.2025. https://www.tenable.com/cybersecurity-guide/learn/key-iam-components. Referenced 20.9.2025.

Tiny Technical Tutorials 2021. AWS Identity and Access Management (IAM) Basics | AWS Training For Beginners. Video. YouTube video service. Published 27.12.2021. https://www.bing.com/videos/riverview/relatedvideo?&q=policy+and+rules+in+iam&qpvt=policy+and+rules+in+iam&mid=AB7B167F2B5C7C1BDBF1AB7B167F2B5C7C1BDBF1&&FORM=VRDGAR. Referenced 30.9.2025.

Tracxn 2025. Aveksa - Company Profile. Online source. Updated 16.6.2025. https://tracxn.com/d/companies/aveksa/__KBQ6NnjlQNJe8D8k7i20vSpYxQWuuQgLG8Ph2vI1jPI#about-the-company. Referenced 16.11.2025.

Tracxn 2025. ClearSkye - About the company. Online source. Updated 2.10.2025. https://tracxn.com/d/companies/clearskye/__9k74pBA4MmXjiHnR6IOnahvpU-vBqCyqnGTM0fVLUUc. Referenced 16.11.2025.

Vuori, J. 2021. Tapaustutkimus. Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/. Referenced 25.10.2025.

APPENDIX 1: IAM SURVEY

* Required

* This form will record your name, please fill your name.

Background questions

1. In which field you are working in the organisation? *

- ◯ HR
- ◯ Finance
- ◯ IT
- ◯ Operations
- ◯ Other

2. In which role you are mainly operating in IDM? *

- ◯ User (seeking access to myself)
- ◯ Manager (seeking and approving access, creating and managing the external subordinates)
- ◯ Role owner
- ◯ Role approver
- ◯ IDM support
- ◯ Auditor

3. How often do you use IDM? *

- ◯ Daily
- ◯ Weekly
- ◯ Occassionally
- ◯ Never

4. What are the most common tasks that you usually perform in IDM? Choose 1-3 options. *

- [ ] Request a new access (including roles and licenses)
- [ ] Search for user information and access details
- [ ] Create an external user
- [ ] Update the contract end date for my external subordinate
- [ ] Request role creation, edition or deletion
- [ ] Other

5. How confident and capable you are in using IDM system? *

1= I don't know how to use IDM. I create an SD ticket if I need to perform something in IDM.
2= I feel unconfident when using IDM.
3= I can perform basic actions in IDM.
4= I can use IDM confidently for most tasks without assistance.
5= I can use IDM independently and efficiently.

1	2	3	4	5

Very unconfident Very confident

6. Briefly explain your previous answer.

Current situation and challenges

7. How satisfied you are with the user experience of the current IDM system (ease of use, clarity and system navigation)? *

1	2	3	4	5

Very unsatisfied Very satisfied

8. Briefly explain your previous answer.

9. How satisfied you're with the technical performance in the current IDM system (speed, reliability and stability)? *

1= The system performance is slow and unreliable which disturbs my work.
2= Some aspects work, but I often face delays and technical problems.
3= The system performance is acceptable, but there are occasional issues.
4= The system performance is relatively fast and stable with only minor disruptions.
5= The system runs smoothly, responds quickly and is reliable.

1	2	3	4	5

Very Unsatisfied Very satisfied

10. Briefly explain your previous answer.

11. What do you experience are the biggest challenges with the current IDM system? Choose 1-3 options. *

- [ ] Tasks in IDM take too long to be completed
- [ ] Automatic user access updates (provisioning) happens too rarely in the IDM system causing delays
- [ ] It is unclear which roles or permissions I need to apply
- [ ] Lack of guidance or support when using IDM
- [ ] Limited visibility to actions history
- [ ] Complex user interface which is hard to navigate
- [ ] Technical issues: access provisions get stuck etc.
- [ ] Other

Values and expectations towards an IDM system

12. How important you consider the following aspects are in an IDM system? *

1=Not important at all, 2=Somewhat important, 3=Neutral, 4=Important, 5=Very important

	Option 1	Option 2	Option 3	Option 4	Option 5
Usability - easy and intuitive user experience	◯	◯	◯	◯	◯
Fast and reliable access provisioning	◯	◯	◯	◯	◯
High fault tolerance and system reliability	◯	◯	◯	◯	◯
Integration with existing systems and platforms	◯	◯	◯	◯	◯
Scalability for future business needs	◯	◯	◯	◯	◯
Strong security and data protection	◯	◯	◯	◯	◯
Transparent and easily accessible traceability of changes and actions	◯	◯	◯	◯	◯
Fast and capable technical support (solving system errors e.g.)	◯	◯	◯	◯	◯
Fast and capable support for requesting access (role, license e.g.)	◯	◯	◯	◯	◯
Visually appealing user interface (style, colours e.g.)	◯	◯	◯	◯	◯

13. What are the most important features in IDM system and why? *

14. What benefits do you expect the most from an identity and access management solution in the future? Choose 1-3 options. *

- [ ] Reduced manual work and more automated features
- [ ] Faster access management
- [ ] Higher fault tolerance
- [ ] Improved information security
- [ ] Seamless integration with other systems and solutions
- [ ] Better user experience
- [ ] More self-service options for users
- [ ] Clearer visibility into roles, permissions and access history
- [ ] Other

15. Any other comments or considerations that should be taken into account when planning the improvement or renewal of an IDM system?