Hochschule Neu-Ulm
University of Applied Sciences

Bachelor Thesis

In the bachelor program

Wirtschaftsinformatik

at the University of Applied Sciences Neu-Ulm

How to manage IAM

First corrector: Prof. Dr. Andy Weeger

Secound corrector: Dr. Anna Wiedemann

Author: Manuel Stevan Yambao (Matrikel-Nr.: 3137083)

Topic received: 16.05.2024

Thesis submitted: 08.09.2024

Digital Appendix

1x ZIP-File

Abstract

This comprehensive study delves into the distinctive characteristics of Identity and Access Management services and their consequential impact on IT Service Management practices. Through a series of qualitative interviews with seasoned professionals from the consulting/audit and re-insurance sectors, the research meticulously examines the unique demands IAM places on ITSM frameworks. The study begins by exploring IAM's unparalleled flexibility in managing user lifecycles, highlighting the dynamic nature of user onboarding and offboarding processes that set IAM apart from other IT services with more static user populations.

A significant revelation from the interviews is the modular design of IAM services, which is paramount for catering to the diverse needs of both internal and external customers. This modularity is not just a feature but a necessity, allowing for tailored solutions that can adapt to the ever-evolving landscape of user requirements. The integration of IAM with enterprise systems emerges as a critical theme, with the study emphasizing the importance of standardized connectors and protocols that enable IAM solutions to integrate seamlessly with a multitude of systems, a demand that is far more pressing than for other IT services.

The implications for ITSM are profound, with the study uncovering the need for elastic resource allocation to accommodate IAM's scalability challenges. Automation, load balancing, and cloud services are identified as essential components to meet these demands, ensuring that IAM services can maintain near-100% availability. This requirement underscores the necessity for robust ITSM processes, including disaster recovery and observability tools, to maintain reliability and prevent service disruptions.

While acknowledging limitations due to methodological choices, scope focus, and sample size, the research paves the way for future work. It calls for a quantitative analysis to complement the qualitative insights and inductive methods to unearth unanticipated relationships between IAM and ITSM. Such an approach would deepen the understanding of IAM services and optimize their deployment within the IT ecosystem, shaping ITSM strategies to meet the unique demands of IAM.

In essence, this thesis provides valuable insights into the distinct nature of IAM services, emphasizing the need for specialized ITSM practices capable of managing their flexibility, modularity, integration, scalability, and availability. It is a clarion call for ITSM frameworks to evolve, ensuring secure and uninterrupted business operations in an increasingly interconnected digital world.

Keywords: Identity and Access Management, IT Service Management, ITSM Framework Adaption, Enterprise System Interoperability, System Integration

Table of Contents

List of Figures

List of Tables

List of Abbreviations

IAM	Identity and Access Management
CIAM	Customer Identity and Access Management
Idm	Identity Management
MFA	Multi-Factor Authentication
RBAC	Role-Based Access Control
SSO	Single Sign-On
SOD	Segregation of Duties
ITIL	ITIL
ITSM	IT-Service Management
PAM	Privileged Access Management
IGA	Identity Governance and Administration

1 Introduction

The rapid advancement of technology has ushered in an era where digital identities are not merely supplementary but as significant as physical identities. This shift underscores the need for a robust and comprehensive framework for managing these digital counterparts. Identity and Access Management (IAM) services have emerged as essential components in the modern digital landscape, playing a critical role in safeguarding and streamlining access to organizational resources. As organizations increasingly rely on digital systems and data, the complexity and importance of managing these identities and their associated permissions have grown exponentially.

This thesis embarks on an in-depth journey to dissect the nuanced distinctions between IAM services and traditional IT services. The objective is to unravel the implications of these distinctions for IT Service Management (ITSM). In an era where digital transformation is reshaping business operations and security paradigms, understanding the unique characteristics of IAM services is crucial. IAM services not only facilitate access control and security but also address compliance and risk management in ways that traditional IT services might not. This differentiation is not merely academic but has tangible impacts on how organizations manage their IT environments and mitigate risks.

The motivation for this inquiry arises from the complex and often intricate web of user access and permissions that modern digital services have woven. Unlike traditional IT services that predominantly focus on infrastructure and applications, IAM services are intrinsically linked to broader themes of security, governance, and compliance. This link means that IAM services directly influence an organization's risk profile and its ability to adhere to regulatory requirements. As digital threats and compliance demands become more sophisticated, the traditional ITSM frameworks may struggle to address the unique challenges posed by IAM.

The potential misalignment between IAM services and established ITSM practices can result in significant security vulnerabilities and operational inefficiencies. For example, traditional ITSM might not fully account for the dynamic and high-stakes nature of identity management, leading to gaps in security or inefficiencies in service delivery. Thus, there is a pressing need to explore how ITSM can evolve to better accommodate the specific demands of IAM services. This thesis is driven by the urgency to shed light on these differences and their broader consequences, aiming to enhance the management of IT services by addressing the distinct and evolving requirements of IAM.

Guiding this exploration are two pivotal research questions: RQ1: How do IAM Services differ from other IT Services? and RQ2: What do these differences imply for IT Service Management? To answer these questions, the research adopts a comparative approach, meticulously examining the attributes of IAM services in contrast to general IT services. This comparative lens helps identify key disparities and challenges.

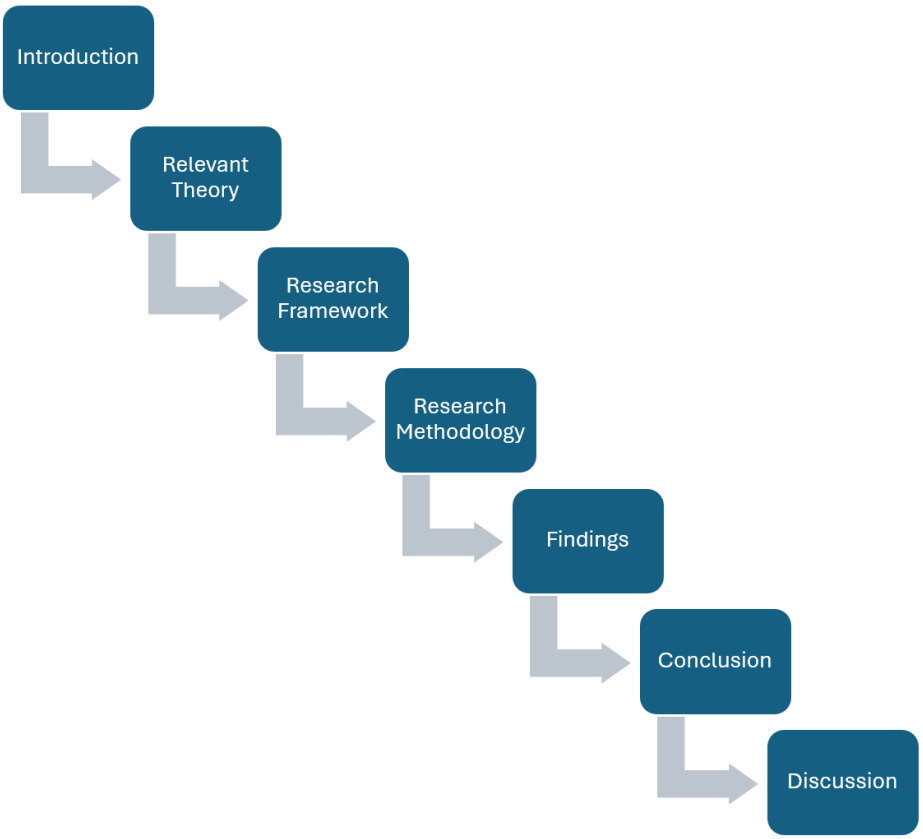

Figure 1: Overview flowchart

The structure of this thesis is meticulously designed to offer a comprehensive exploration of the research topic, guiding the reader through each stage of the investigation from theoretical foundations to the presentation of findings.

The journey begins with the **Introduction**, which establishes the research context by detailing the motivation behind the study. This chapter introduces the core research questions and underscores the importance of understanding how IAM services differ from traditional IT services, as well as the implications of these differences for ITSM By laying this foundational groundwork, the introduction aims to highlight the relevance and urgency of the research.

Following this, the **Relevant Theory** chapter delves into the theoretical concepts crucial for grasping the complexities of IAM and ITSM. It provides an in-depth review of IAM components, including Identity Management, Access Management, Privileged Access Management, Customer Identity and Access Management, IAM Federation, and IAM Characteristics. Each section meticulously covers these aspects, offering a comprehensive understanding of their roles within IAM. In parallel, the chapter explores essential ITSM concepts such as Availability Management, ITSM Scalability, and Service Modularity. This section reviews fundamental theories and practices of ITSM, examining their relevance to IAM services. The chapter also identifies existing research gaps, framing the study by highlighting areas that warrant further investigation.

The **Research Framework** chapter revisits the research questions and assumptions, outlining the framework guiding the study. It features a detailed description of the research framework and includes a diagram illustrating the presumed relationships between IAM and ITSM. This visual representation aids in understanding the proposed assumptions and their connections.

In the **Research Methodology** chapter, the methodology for addressing the research questions is outlined. This chapter describes how the interviewees were selected, the design of the questionnaire, and the data collection process. It provides a transparent account of the methods used to gather and analyze data, including the rationale behind the selection of interviewees and the procedures followed during the interviews.

The **Findings** chapter presents the results derived from the data analysis, examining how the insights obtained from the interview transcripts relate to the research assumptions. This chapter offers a detailed discussion of the evidence, highlighting how it supports or refutes the assumptions.

The **Conclusion** chapter synthesizes the key findings and provides answers to the research questions based on the evaluated Assumptions. It summarizes the main results and their implications for IAM and ITSM, offering a clear overview of the study's contributions.

Finally, the **Discussion** chapter reflects critically on the entire thesis, addressing the study's limitations and proposing directions for future research. This chapter aims to deepen the understanding of the interplay between IAM and ITSM and to suggest further areas for exploration.

Overall, this structure ensures a thorough and coherent examination of the research topic, guiding the reader through the theoretical foundations, research methods, findings, and their implications in a clear and systematic manner.

2 Relevant Theory

2.1 Introduction into IAM

Identity and Access Management (IAM) is a framework of policies and technologies that ensures the right individuals access the appropriate resources at the right times for the right reasons. IAM systems provide secure and efficient management of user identities and access privileges within an organization (Bertino, 2010).

IAM is critical in modern IT environments due to the increasing complexity and distributed nature of IT infrastructures. It involves not only the management of individual user identities but also the processes and technologies used to manage access to systems, applications, and data (ISO/IEC 27001, 2013). IAM encompasses a wide range of functions, including user authentication, authorization, user lifecycle management, and the monitoring and auditing of access activities (NIST, 2019).

Core components / services of IAM include:

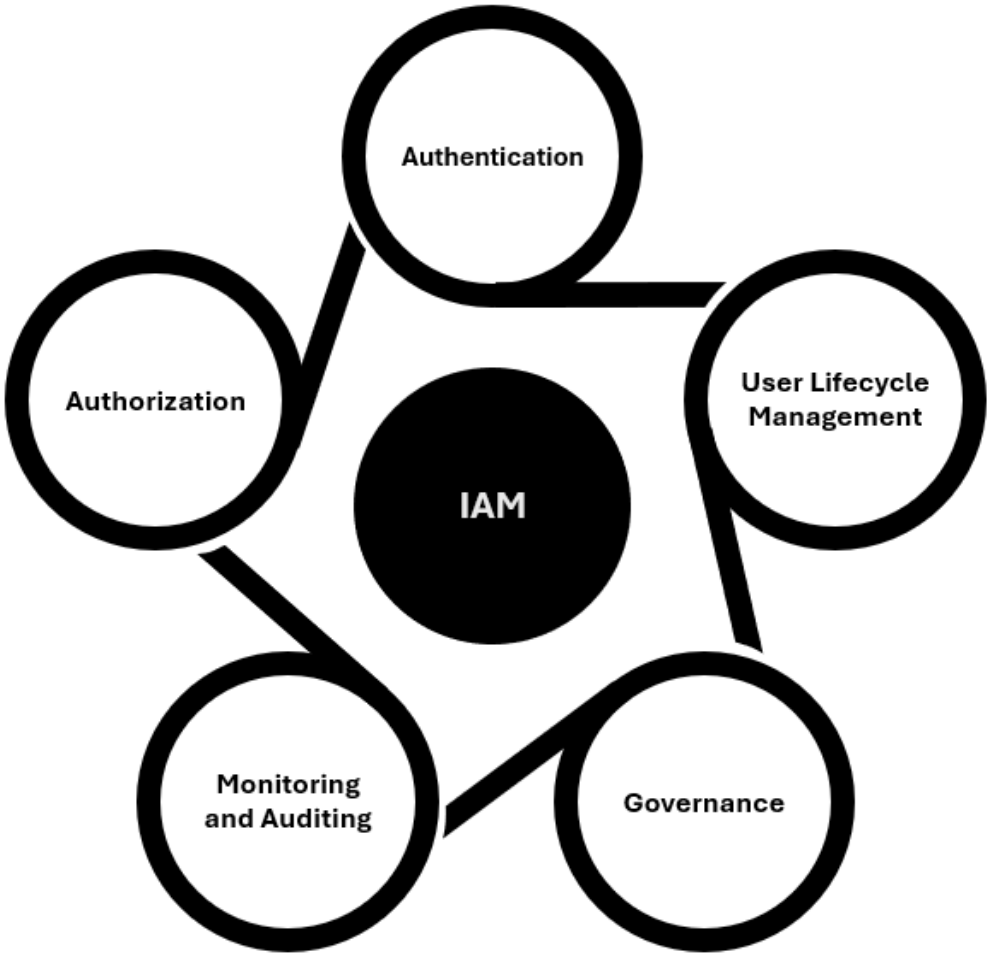

Figure 2: IAM Components

Authentication: This process verifies the identity of a user attempting to access a system. Authentication mechanisms include passwords, biometric scans, and multi-factor authentication (MFA), which

combines multiple verification methods to enhance security (O'Gorman, 2003). For instance, every morning, an employee might log into their computer using a password and then receive a text message with a one-time code to access the company's VPN, ensuring that their identity is securely confirmed before starting work.

Authorization: Once a user's identity is authenticated, authorization determines what resources the user can access and what actions they are permitted to perform. Role-Based Access Control (RBAC) is a common authorization strategy that assigns permissions to users based on their roles within the organization (Ferraiolo & Kuhn, 1995). For example, a sales representative may be authorized to view customer contact information and sales records, but not to access the company's financial reports, which are restricted to the finance department's staff.

User Lifecycle Management: This involves the processes for creating, managing, and deleting user accounts and access privileges throughout the lifecycle of a user's relationship with the organization. Effective lifecycle management ensures that access rights are appropriately granted and revoked in response to changes in a user's status (Bertino, 2010). When an employee is promoted, the IT department updates their account to grant access to new systems and data relevant to their new role, while revoking permissions that are no longer necessary.

Access Governance: This component involves policies and processes to ensure that access rights are consistent with organizational policies and regulatory requirements. Access governance includes regular audits and reviews of user access rights to identify and mitigate risks (ISO/IEC 27001, 2013). An annual audit might reveal that some employees still have access to a project management tool long after their projects have concluded, prompting a review and adjustment of their access rights to align with current needs and security policies.

Monitoring and Auditing: Continuous monitoring and periodic auditing of access activities help detect and respond to security incidents. Monitoring tools track user activities in real-time, while audits provide historical analysis to ensure compliance with security policies (NIST, 2019). For example, a security team may receive an alert when a user attempts to access a restricted area of the company's intranet, triggering an investigation to determine whether this was an innocent mistake or a potential security breach.

IAM provides several benefits, including enhanced security by ensuring that only authorized individuals access sensitive resources, reducing the risk of security breaches and insider threats (Bertino, 2010). IAM also helps organizations comply with regulatory requirements by providing mechanisms to enforce and demonstrate compliance with data protection and privacy regulations (ISO/IEC 27001, 2013). Additionally, it increases operational efficiency by automating processes that reduce the administrative burden of managing user identities and access rights, freeing up IT resources for other tasks (NIST, 2019). IAM solutions, such as Single Sign-On (SSO), also improve user experience by allowing users to access multiple applications with a single set of credentials (O'Gorman, 2003).

Despite its benefits, IAM implementation can be challenging. Organizations may face difficulties integrating IAM solutions with existing systems, managing the complexity of access controls, and keeping up with evolving security threats. Effective IAM requires a strategic approach that includes comprehensive planning, stakeholder involvement, and continuous evaluation and improvement (Bertino, 2010).

In this chapter, we endeavor to provide a comprehensive introduction to IAM and its associated subservices, aiming to elucidate the distinct requirements that IAM imposes on an ITSM framework. Despite the multifaceted diversity inherent in IAM, the discourse herein is designed to furnish a foundational understanding of both IAM and ITSM. The topics delineated are intended to facilitate comprehension for subsequent evaluation and to offer a general perspective on the intricate interplay between IAM and

ITSM. This foundational overview serves as a steppingstone for readers to gain a better understanding of the critical role that IAM plays within the broader context of ITSM.

2.1.1 Identity Management

Identity Management (IdM) is a critical component of Information Technology security that focuses on managing and securing user identities within an organization. It encompasses the processes, policies, and technologies used to manage the lifecycle of digital identities, ensuring that the right individuals have the appropriate access to resources and information (Bertino, 2010). In today's interconnected and digitally driven world, the importance of Identity Management cannot be overstated. As organizations adopt more complex IT infrastructures, including cloud services and remote work environments, the need for robust identity management systems has become paramount (ISO/IEC 27001, 2013). Identity Management is essential for maintaining the security of an organization's data and systems by preventing unauthorized access and ensuring compliance with regulatory requirements (NIST, 2019).

Core components of Identity Management include user provisioning and de-provisioning, authentication, authorization, directory services, SSO and Identity Governance and Administration (IGA) which can be executed via IGA-Tools.

2.1.2 Access Management

Access Management is a fundamental component of IAM, focusing on regulating user access to systems, applications, and data within an organization. This process ensures that authenticated users receive the appropriate level of access needed to perform their roles, while simultaneously protecting sensitive information from unauthorized access. Access Management involves implementing policies and technologies that define and enforce access control mechanisms. Role-Based Access Control is a widely adopted model that simplifies access management by assigning permissions to roles rather than individuals, thereby streamlining the process and reducing administrative overhead. By leveraging these techniques, organizations can enhance security, improve operational efficiency, and ensure compliance with regulatory requirements. The dynamic nature of modern IT environments necessitates robust and adaptive access control mechanisms to address evolving security challenges and safeguard organizational assets (Ferraiolo & Kuhn, 1992).

2.1.3 Role Based Access Control

Building upon the principles of Access Management, Role-Based Access Control (RBAC) is a pivotal model that significantly enhances the efficiency and security of access control mechanisms within organizations. Introduced by Ferraiolo and Kuhn, RBAC operates by assigning access permissions based on the roles within an organization rather than to individual users directly. This approach simplifies the management of user permissions, as roles are typically aligned with job functions, ensuring that users have access only to the resources necessary for their role. By centralizing permissions management through roles, RBAC reduces the complexity and potential errors associated with individual access assignments. This model not only streamlines administrative processes but also strengthens security by ensuring consistent enforcement of access policies across the organization. Consequently, RBAC has become a widely adopted standard in modern IT environments, particularly in complex and large-scale systems where managing individual access rights would be impractical (Ferraiolo & Kuhn, 1995).

2.1.4 Privileged Access Management

Privileged Access Management (PAM) is an essential security measure designed to protect an organization's critical assets from unauthorized access and potential security breaches. PAM solutions are built to restrict and monitor the activities of users with elevated permissions, who have the ability to significantly impact the IT environment. By implementing stringent access controls and continuous surveillance of privileged operations, PAM systems ensure that only authorized personnel can access sensitive systems and data. This is particularly crucial in mitigating risks stemming from both external threats and insider vulnerabilities. The introduction of PAM into an organization's security strategy is a proactive step towards maintaining the confidentiality, integrity, and availability of data, which are the foundational principles of information security. This thesis will examine the fundamental aspects of PAM, its importance in the modern security landscape, and the best practices for its implementation to safeguard against the ever-present threat of cyber attacks (Tep,Martini,Hunt & Choo, 2015).

2.1.5 Customer Identity and Access Management

Customer Identity and Access Management (CIAM) has emerged as a critical area of focus in the realm of digital interactions between individuals and organizations. This framework encompasses the processes and technologies designed to facilitate secure and efficient interactions, particularly in the digital space. With the increasing reliance on online platforms for a range of activities—from commercial transactions to accessing social services—CIAM plays a pivotal role in managing how individuals identify themselves and interact with digital services (Glazer, 2023).

CIAM is distinct from traditional workforce Identity and Access Management (IAM) in several key aspects. While both fields involve managing identities and access, CIAM focuses on the unique challenges associated with customer interactions. This includes ensuring secure registration, authentication, and authorization processes tailored to a diverse user base. The goal of CIAM is not only to protect sensitive information but also to enhance user experience and support organizational objectives, such as expanding reach and reducing service delivery costs (Glazer, 2023).

In the evolving digital landscape, CIAM is essential for organizations aiming to deliver personalized and secure customer engagements. This chapter explores the fundamental concepts of CIAM, highlights its differences from workforce IAM, and examines the implications of its implementation for both public and private sector entities. By understanding CIAM, organizations can better navigate the complexities of digital identity management and leverage its benefits to build trust and foster lasting customer relationships (Glazer, 2023).

2.1.6 IAM Federation

In the context of IAM, federation refers to the linking of several distinct identity management systems. Federated identity management allows a user's single authentication ticket, or token, to be trusted across multiple IT systems or even organizations. This means that a user can authenticate once (SSO) and gain access to the resources of multiple software systems. This is particularly useful in scenarios where users need to interact with multiple services or websites that have trust relationships, allowing them to sign in just once and use all the related services without needing to reauthenticate. (Jensen, 2012)

2.1.7 Segregation of Duties

Segregation of Duties (SoD) is a critical principle in organizational governance, aimed at preventing fraud and ensuring the integrity of processes by requiring that no single individual has control over all parts of a critical function. The innovative model proposed by Kobelsky (2014) underscores the necessity of involving multiple individuals in IT processes to enhance security and operational effectiveness. By differentiating specific duties and assigning them across a team, organizations can tighten security controls and align with the demands of modern automated systems. The model advocates for a minimum of three individuals to be involved in IT processes to maintain proper SoD, highlighting the significance of secondary authorizations and account reconciliations in the framework. This comprehensive approach seeks to reconcile the practical challenges of applying SoD with the theoretical underpinnings, offering substantial improvements for organizations looking to optimize their systems without compromising control quality or cost-efficiency (Kobelsky, 2014).

To illustrate the principle of SoD, consider the example of a sales cycle within an organization. SoD dictates that the tasks of setting prices, authorizing transactions, and handling customer payments should be performed by different individuals. For instance, if a salesperson sets the price for a sales order, another employee should be responsible for authorizing that price, and a third should handle the receipt of payment. This division of responsibilities helps to prevent any single person from having the opportunity to both commit and conceal an error or fraudulent activity, thereby safeguarding the organization's assets and maintaining the integrity of its processes (Kobelsky, 2014).

2.1.8 IAM Characteristics

With a foundational understanding of IAM established, it is essential to delve into the specific characteristics that define and differentiate IAM systems. These characteristics are crucial for comprehending how IAM systems function and their importance in securing organizational environments. The following sections will explore key aspects of IAM, including user number flexibility, resource requirements, criticality, customer needs, and the level of integration required. Each of these characteristics plays a significant role in shaping the effectiveness and efficiency of IAM solutions. By examining these elements, we gain deeper insights into how IAM systems adapt to dynamic user environments, manage resources, uphold critical security measures, cater to diverse customer requirements, and integrate seamlessly with various applications and services. Understanding these aspects not only provides a comprehensive view of the operational demands and strategic importance of IAM but also sets the stage for developing key assumptions in the subsequent chapter.

User number flexibility

User number flexibility is essential in IAM as it allows organizations to efficiently manage access for varying numbers of users, whether due to changes in workforce size or shifts in project demands. This flexibility is particularly important in cloud environments, where the number of users may frequently change. A flexible IAM system ensures that security is maintained without unnecessary complexity or cost, as it can dynamically scale up or down. Additionally, this flexibility supports compliance efforts by ensuring that access controls can be promptly adjusted to meet regulatory requirements (Jansen & Grance, 2011)

Resource Requirements

Understanding resource requirements is crucial for effective IAM because it ensures that the system can support the necessary security functions without overloading. Adequate resource allocation allows IAM systems to handle the demands of user authentication, access controls, and monitoring, which are essential for maintaining security in large or complex environments. For instance, NIST Special Publication 800-53 outlines the importance of ensuring that IAM systems have sufficient resources to implement security controls effectively, such as processing power and storage for maintaining access logs and executing security protocols (NIST, 2020). Additionally, the NIST Cybersecurity Framework emphasizes the need for resource management within the "Protect" function, which includes access control and identity management as key components, ensuring that these systems remain resilient against threats (NIST, 2018).

Criticality:

IAM is critical to organizational security because it serves as the backbone for controlling and protecting access to sensitive information and systems. Effective IAM ensures that only authorized users can access specific resources, thereby mitigating risks associated with unauthorized access and data breaches. This criticality is underscored by the need for robust IAM systems to enforce security policies, manage user identities, and handle authentication and authorization processes effectively. According to the National Institute of Standards and Technology (NIST), IAM systems are vital for maintaining security and compliance, as they directly impact an organization's ability to safeguard its assets and adhere to regulatory requirements (NIST, 2020).

Customer Need:

IAM systems must address varying customer needs regarding authentication methods and integration approaches. Applications and resources often require different types of authentication to balance security and user convenience. For example, cloud applications frequently demand support for modern authentication techniques such as SSO and MFA to enhance security and provide a seamless user experience across multiple services (Mell & Grance, 2011). In contrast, enterprise applications may need IAM systems to integrate with existing directory services like Active Directory or LDAP, which is crucial for managing user identities and permissions within established organizational frameworks (NIST, 2018). These differences underscore the need for IAM solutions that are adaptable to various authentication methods and integration requirements.

Higher Level of Integration:

To effectively onboard a variety of applications and services, IAM systems must have a high degree of integration. This integration is crucial for enabling features such as SSO and MFA across diverse platforms, which improves both security and user convenience. As organizations increasingly adopt complex IT environments, including cloud and hybrid solutions, IAM systems must integrate seamlessly with various applications to ensure centralized management of user identities and consistent security policy enforcement (NIST, 2020).

2.2 Introduction into IT Service Management

Having established the foundational principles of IAM, this thesis now turns its focus to ITSM. This shift in attention is pivotal for comprehending the rationale behind the detailed exposition of certain aspects of ITSM over others within the scope of this study, particularly those that exert a more significant impact on the thematic areas under consideration. This approach is deliberately selective, addressing only the most salient facets of ITSM to facilitate a better understanding of the subsequent content and to maintain a concentrated examination of the most influential elements.

ITSM refers to the entirety of activities, processes, and policies used by an organization to design, deliver, manage, and improve IT services. ITSM emphasizes aligning IT services with the needs of the business, ensuring that the right processes, people, and technology are in place to support organizational goals (Galup et al., 2009).

It is a strategic approach to designing, delivering, managing, and improving the way IT is used within an organization. Unlike other IT management disciplines that focus on hardware, networks, or systems, ITSM is primarily concerned with customer-facing services and ensuring that these services are provided in a quality-driven and cost-effective manner (Axelos, 2019). This approach ensures that IT services support and enhance the business processes they are intended to facilitate (Office of Government Commerce, 2007).

Core components of ITSM include well-defined processes and best practices, such as Incident Management, Problem Management, Change Management, Service Request Management, and Service Level Management. These processes help maintain service quality and manage risk (Galup et al., 2009). Additionally, several frameworks and standards guide ITSM practices, with the Information Technology Infrastructure Library (ITIL) being the most widely recognized. Other notable frameworks include COBIT (Control Objectives for Information and Related Technologies) and ISO/IEC 20000, an international standard for ITSM (Office of Government Commerce, 2007; IT Governance Institute, 2007).

ITSM encompasses the entire lifecycle of IT services, from initial service strategy and design through to transition, operation, and continual improvement. This lifecycle approach ensures that services are continuously aligned with business needs and can adapt to changing requirements (Axelos, 2019). Effective ITSM relies on various tools and technologies that support the automation of processes, help manage IT assets, and provide analytics and reporting, enhancing efficiency, transparency, and accountability within the IT service delivery process (Galup et al., 2009).

The adoption of ITSM practices offers numerous benefits, including improved efficiency through standardized processes and automated workflows, enhanced service quality by following best practices and frameworks like ITIL, increased agility in responding to changes in business requirements and technological advancements, cost savings through optimized IT operations and resource utilization, and better risk management with structured processes for change and incident management (Galup et al., 2009; Marrone & Kolbe, 2011).

However, implementing ITSM can present several challenges, such as resistance to change, the need for significant upfront investment in tools and training, and the complexity of aligning ITSM processes with existing business processes (Hochstein et al., 2005). Organizations must carefully plan their ITSM strategy and foster a culture of continuous improvement to realize its full benefits (Hochstein et al., 2005; Marrone & Kolbe, 2011).

In conclusion, ITSM is a crucial component of modern IT operations, providing a structured approach to managing and delivering IT services that align with business objectives. By implementing best practices and frameworks like ITIL, organizations can enhance service quality, improve efficiency, and achieve better alignment between IT and business goals (Axelos, 2019; Office of Government Commerce, 2007).

Following the overall introduction to this thesis, which establishes the foundational context for understanding IAM services and their significance, the focus will only be more detailed examined for specific fields within ITSM. This is necessary because certain aspects of ITSM play a particularly pivotal role in the management and operation of IAM services. In the upcoming sections, we will explore in greater detail those ITSM domains that are especially relevant to IAM services such as availability management, scalability, and modularity which have been chosen due to their impact from characteristics of IAM. By delving into these areas, this thesis aims to elucidate how these ITSM practices are tailored to address the unique challenges and requirements posed by IAM services, thereby offering an understanding of their impact and implications for effective ITSM.

2.2.1 Availability Management

Availability management is a critical discipline within ITSM that focuses on ensuring the continuous and reliable operation of IT services. Its primary objective is to minimize service downtime and maximize service availability, which is essential for maintaining business continuity and meeting user expectations (Limoncelli, Chalup, & Klein, 2007). In the realm of ITSM, availability management involves the implementation of strategies and practices to proactively manage and mitigate potential disruptions, ensuring that services are consistently available as per agreed-upon service levels (Axelos, 2021).

2.2.2 ITSM Resource Management

ITSM Resource Management is a critical process within ITSM that focuses on the efficient and effective management of IT resources to ensure that they are allocated and utilized in alignment with organizational goals and service requirements. This process involves the planning, coordination, and control of resources such as personnel, hardware, software, and financial assets to support IT service delivery and projects. Effective resource management ensures that the right resources are available at the right time, reducing inefficiencies and optimizing resource usage to enhance service quality and operational performance. It is integral to ensuring that IT services are delivered reliably and efficiently, meeting the demands of the business and contributing to overall organizational success (Axelos, 2019).

2.2.3 ITSM Scalability

Scalability is a fundamental aspect of modern ITSM and IT services. It refers to the capability of a system to handle a growing amount of work, or its potential to accommodate growth. In the context of ITSM and IT services, scalability ensures that the services provided by an organization can grow and evolve in response to increasing demands without compromising performance or quality.

Scalability within ITSM is crucial for several reasons. As businesses grow, their IT needs expand, and scalable ITSM processes ensure that IT services can support this growth without requiring a complete overhaul of existing systems (Galup, Dattero, Quan, & Conger, 2009). Efficient scalability helps in optimizing resources by ensuring that IT services can handle increased loads with minimal waste, which is

especially important in environments where resources are billed based on usage, such as cloud computing (Marinescu, 2017). Additionally, scalable ITSM processes help maintain service continuity and performance during peak loads or unexpected increases in demand, which is essential for maintaining customer satisfaction and trust (Axelos, 2019). Implementing scalability in IT services can involve leveraging the benefits of cloud computing, where services can automatically scale to meet demand, providing additional resources as needed and scaling down when demand decreases (Armbrust et al., 2010). However, it is important to note that cloud computing is an option and not a must; organizations can also achieve scalability through other means such as on-premises infrastructure improvements and hybrid solutions. To implement scalability effectively, continuous monitoring and performance management are necessary, and tools and techniques such as load balancing, auto-scaling, and resource monitoring play a vital role in ensuring that IT services can scale in response to real-time demand (Kavis, 2014). By leveraging these tools, organizations can detect potential bottlenecks and take proactive measures to address them.

2.2.4 Service Modularity

Service Modularity is defined as the structuring of services into distinct components or modules that can be independently created, modified, replaced, and reused. These modules can be combined in various ways to create customized service offerings, allowing for greater flexibility and efficiency in service design and delivery. The concept is adapted from product design and applied to services, and it is associated with several key benefits, including the reduction of complexity, improved transparency, enhanced improvement and reuse of modules, and the ability to structure individual services for configuration (Doehrbecker & Boehmann, 2013)

2.3 Research GAP

In this chapter, we have established a foundational understanding of IAM and ITSM. IAM is essential for managing and securing user identities and access within organizations, focusing on core components such as authentication, authorization, user lifecycle management, and access governance. Key characteristics of IAM, such as flexibility in managing user numbers, resource requirements, and the necessity for high levels of integration, are vital for adapting to the dynamic needs of modern IT environments. Conversely, ITSM involves the design, delivery, management, and improvement of IT services to align with business needs. Core ITSM practices include resource management, availability management, service delivery with a focus on scalability, and modularity. The key characteristics of IAM outlined will help in formulating assumptions that will be tested to answer the thesis's research questions.

Despite the extensive literature on IAM services and the well-established documentation on ITSM practices, a notable research gap exists in the integration of IAM services within the broader framework of ITSM. While numerous studies have explored the specific requirements and challenges of IAM services from the perspective of customer needs, and a substantial body of work details various ITSM practices (Axelos, 2019), there is a lack of comprehensive research that bridges these two domains. Specifically, there is insufficient exploration into how IAM services intersect with and impact ITSM practices, including aspects such as availability management, scalability, and integration. This gap signifies a critical area for investigation, as understanding how IAM services align with ITSM principles and processes is essential for optimizing their management and operation. This thesis aims to address this gap by examining how IAM services differ from other IT services and what these differences imply for effective ITSM, thereby contributing valuable insights to both fields.

3 Research Framework

3.1 Research Question and Assumption

The research conducted in this thesis revolves around two primary questions aimed at exploring the unique characteristics and implications of IAM services in comparison to other IT services. These research questions are designed to guide the investigation and provide a structured approach to understanding the complexities of IAM services within the broader context of ITSM. The central research questions are as follows:

RQ1: How do IAM Services differ from other IT Services?

RQ2: What do these differences imply for IT Service Management?

To address these research questions comprehensively, several assumptions have been formulated. These assumptions are grounded in the premise that IAM services exhibit distinct characteristics compared to other IT services and that these differences have significant implications for ITSM. The assumptions were developed based on a detailed analysis of the unique characteristics of IAM services, which include their flexibility, scalability, criticality, modularity, and integration requirements. The following assumptions guide the investigation:

Assumption 1 (A1): IAM services differ from other IT services due to their high user number flexibility, which arises from frequent application onboarding and offboarding processes.

This assumption posits that the inherent flexibility of IAM services, necessitated by the frequent addition and removal of applications and user access requirements, distinguishes them from other IT services. This flexibility is crucial for adapting to the dynamic and evolving needs of both users and organizations, highlighting the unique operational demands placed on IAM services.

Assumption 2 (A2): The resource scalability requirements of IAM services, due to variable user loads, imply that IT service management must focus on elastic resource allocation.

According to this assumption, the need for IAM services to accommodate fluctuating user loads necessitates a focus on scalable and elastic resource management. Effective ITSM for IAM services must incorporate strategies for dynamic resource allocation to handle varying demands efficiently, ensuring that resources are optimally distributed in response to changing usage patterns.

Assumption 3 (A3): The criticality of IAM services necessitates a highly effective availability management that includes specific mechanisms to ensure service continuity.

This assumption suggests that due to the pivotal role IAM services play in maintaining secure access and operations, they require stringent availability management practices. Effective management must

include specific mechanisms to ensure uninterrupted service and continuity, reflecting the high stakes involved in ensuring that IAM services are always reliably available.

Assumption 4 (A4): IAM services offer a variety of subservices, requiring a modular service design to meet the diverse needs of both internal and external customers.

This assumption asserts that the diverse array of subservices provided by IAM solutions necessitates a modular design approach. This modularity is essential for addressing the varied requirements of different user groups and ensuring that both internal and external customer needs are effectively met, allowing for tailored solutions within a unified framework.

Assumption 5 (A5): IAM services require a higher degree of integration with other enterprise systems compared to other IT services, which implies that ITSM must prioritize interoperability and standardized protocols.

This assumption highlights the need for IAM services to seamlessly integrate with other enterprise systems. It implies that effective ITSM for IAM services must prioritize interoperability and adhere to standardized protocols to ensure smooth integration and operational efficiency, addressing the complexities of connecting diverse systems and applications within an organization.

A deductive approach has been chosen for this research, meaning that these assumptions will be systematically tested throughout the thesis. To validate or refute these assumptions, the research will employ interviews as the primary method of data collection. Through structured interviews with experts in the field, the research aims to gather empirical evidence and insights that will either support or challenge the formulated assumptions. This structured examination will help elucidate how the unique characteristics of IAM services necessitate specific adaptations in ITSM practices and identify key areas where ITSM frameworks may need to evolve to better support the distinctive requirements of IAM services.

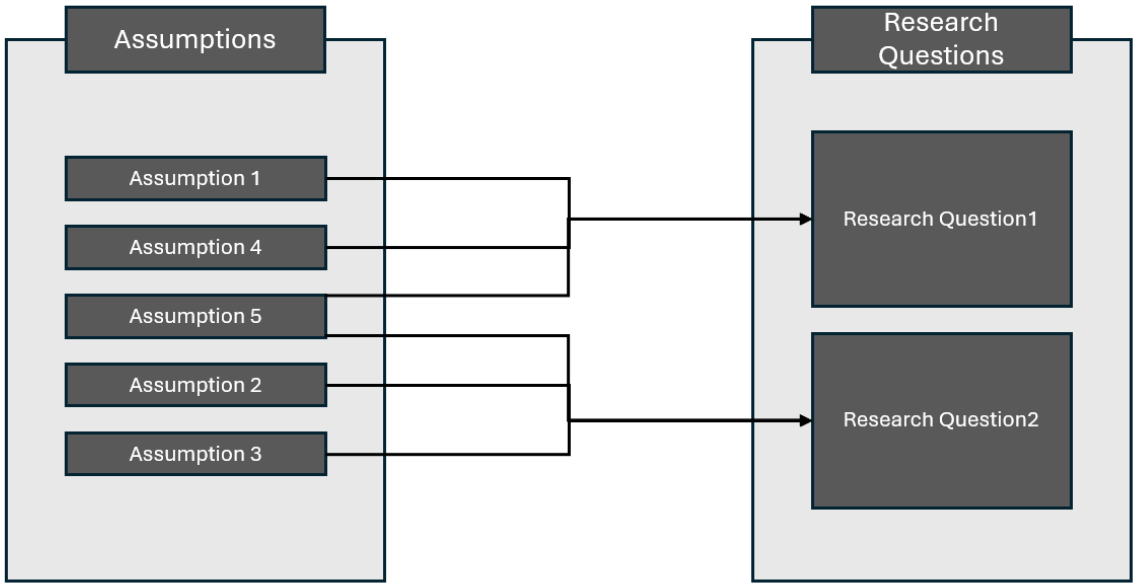

Figure 3: Assumption - Research Question Mapping

To provide a more comprehensive understanding of how the assumptions relate to the research questions, it is useful to refer to the accompanying figure, which visually maps out these connections. This visual representation illustrates how each assumption interlinks with the broader research objectives, offering a clearer picture of the relationships at play.

Assumption 1 (A1), Assumption 4 (A4), and Assumption 5 (A5) are particularly relevant to Research Question 1 (RQ1). RQ1 seeks to explore the specific ways in which IAM services differ from other IT services. Assumption 1 (A1) examines the high user flexibility inherent in IAM services due to their frequent application onboarding and offboarding processes. This assumption underscores the distinctive operational demands of IAM services compared to traditional IT services. Assumption 4 (A4) focuses on the necessity of a modular service design within IAM services, which is driven by the diverse needs of both internal and external customers. This modularity is a critical aspect of how IAM services stand apart from other IT services. Assumption 5 (A5) also falls under RQ1 as it highlights the higher degree of integration required by IAM services with other enterprise systems. This integration aspect differentiates IAM services from other IT services by demonstrating the unique technical requirements of IAM systems.

On the other hand, Assumptions 2 (A2), 3 (A3), and 5 (A5) are directly relevant to Research Question 2 (RQ2), which addresses the implications of these differences for ITSM. Assumption 2 (A2) explores the scalability requirements of IAM services, emphasizing the need for elastic resource allocation to manage variable user loads. This assumption reflects the broader implications for ITSM, as it points to the necessity for adaptable resource management strategies in response to IAM-specific demands. Assumption 3 (A3) discusses the criticality of IAM services and the need for highly effective availability management to ensure service continuity. This assumption highlights the importance of robust ITSM practices to support the critical nature of IAM services. Notably, Assumption 5 (A5) also pertains to RQ2, as it not only addresses the unique integration needs of IAM services but also informs ITSM practices by underscoring the importance of interoperability and standardized protocols in managing these services effectively.

3.2 Research Framework Diagram

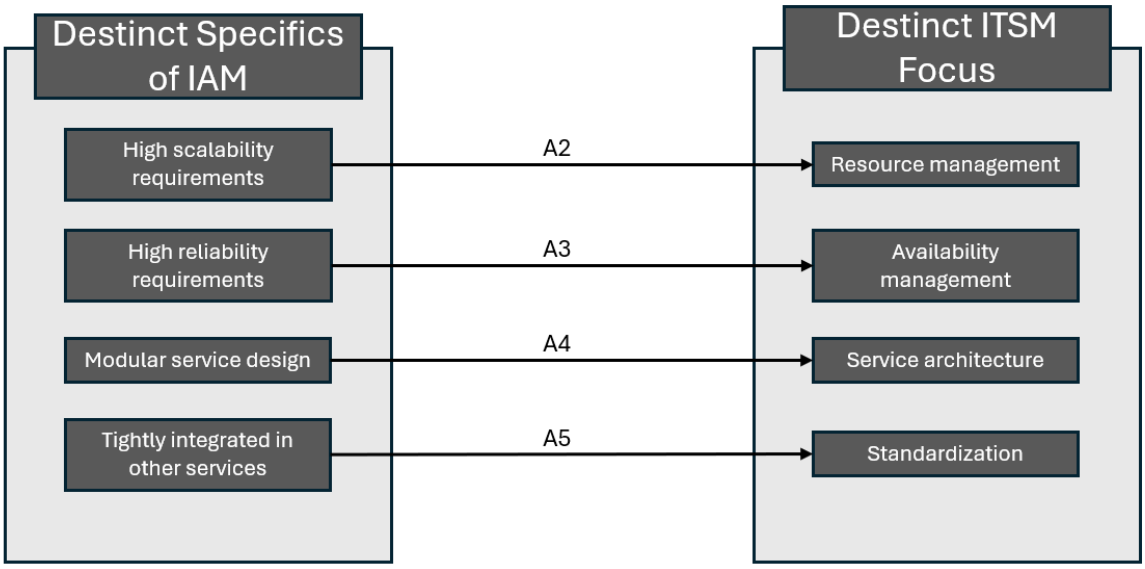

Figure 4: Research Framework Diagram

The research framework is depicted in a diagram that illustrates the relationship between the unique characteristics of IAM services and their corresponding implications for ITSM. The diagram is organized into two primary sections: "Distinct Characteristics of IAM" and "Distinct ITSM Focus." This structure visually represents how the specific attributes of IAM services influence and necessitate particular areas of focus within ITSM.

On the left side of the diagram, the distinct characteristics of IAM services are presented. These include the high scalability requirements, which are driven by the necessity to manage varying user loads due to the dynamic nature of access needs within organizations. This characteristic implies that ITSM must prioritize elastic resource management to ensure that resources can be adjusted according to fluctuating demands. Additionally, IAM services require a high degree of reliability, making effective availability management a critical focus for ITSM to guarantee continuous and secure service delivery. The modular service design of IAM, which often involves multiple subservices tailored to diverse customer needs, necessitates that ITSM pays close attention to maintaining this modular architecture. This focus ensures that the different components of IAM services work seamlessly within the broader IT infrastructure. Moreover, IAM services demand a higher degree of integration with other enterprise systems, highlighting the importance of standardization within ITSM to facilitate interoperability and consistent service quality across various platforms.

On the right side of the diagram, the corresponding ITSM focus areas are illustrated. Resource management emerges as a key focus, driven by the scalability demands of IAM services. Similarly, the need for high reliability in IAM services requires a strong emphasis on availability management within ITSM. The modular nature of IAM services directly influences ITSM's focus on service architecture, ensuring that the modularity of IAM systems is preserved and effectively managed. Finally, the necessity for tight

integration with other services underscores the importance of standardization within ITSM, which is essential for achieving interoperability and maintaining consistent service delivery across different systems.

The diagram uses labeled arrows to connect the unique characteristics of IAM with the corresponding ITSM focus areas, with each arrow representing a specific assumption that links these aspects. This visual representation highlights the intricate relationship between the distinct features of IAM services and the ITSM practices needed to manage them effectively.

4 Research Methodology

In addressing the research questions posed in this study a qualitative deductive approach has been deemed most appropriate. This methodological choice is grounded in the recognition that the subject matter requires an in-depth exploration of complex, context-dependent phenomena that quantitative methods may not adequately capture.

Qualitative research is particularly well-suited to answering 'how' and 'what' questions, as it allows for a deep understanding of human behavior, experiences, and the reasons that govern such behavior (Bryman, 2016). The nuanced differences between IAM services and other IT services, as well as their implications for IT service management, are best explored through a method that can capture the subtleties of these distinctions.

The deductive component of this approach involves developing a conceptual framework based on existing knowledge and theories, and then applying this framework to the empirical world (Bryman, 2016). In this study, the deductive approach allows for the application of general theories of IT service management to the specific case of IAM services. This structured approach facilitates the examination of whether the theoretical propositions hold true in the particular context of IAM services.

One of the key advantages of a deductive approach in qualitative research is its capacity to test and potentially extend theoretical propositions within a new or specific context. By applying established theories to the case of IAM services, this study can contribute to the broader literature on IT service management by confirming, refining, or challenging the existing theoretical framework.

Moreover, a qualitative deductive approach enables the researcher to gather rich, detailed data that can provide insights into the perceptions and experiences of individuals involved with IAM services. This approach is particularly pertinent to the second research question, which seeks to understand the broader implications of the differences identified. Through qualitative data collection methods such as interviews, the study can delve into the complexities and practical considerations that shape the management of IAM services.

In conclusion, the qualitative deductive approach was selected for its alignment with the research questions and its ability to provide a thorough and nuanced understanding of the differences between IAM services and other IT services, as well as their implications for IT service management. This approach, supported by the literature on qualitative research methods (Bryman, 2016), ensures that the study is both methodologically sound and rich in empirical content.

4.1 Selection of Interviewees

For the interviews conducted in this research, professionals were selected from two distinct companies to ensure a comprehensive exploration of IAM services and their implications for ITSM. This approach was designed to capture a broad range of perspectives and areas of expertise, facilitating a well-rounded understanding of the unique characteristics and challenges associated with IAM services. The professionals selected represented a variety of roles and specializations, contributing to a nuanced analysis of IAM in comparison to other IT services.

Company Type	*Number of Employees*	*Description*	*Number of Interviews*
Consulting / Audit	395.442	The company is a global professional services firm that offers a broad range of services including advisory, assurance, tax, and transaction services. With a strong international presence, the firm operates in numerous countries and serves a diverse clientele, including multinational corporations, small and medium-sized enterprises, and governmental entities. The company's core competencies lie in providing expert consulting on business strategy, financial performance, risk management, and regulatory compliance.	4
Re-Insurance	39.662	The company is a leading global reinsurance provider with a strong presence in the international insurance market. It specializes in offering reinsurance solutions and risk management services to insurance companies and other financial institutions worldwide. The firm's expertise spans various areas, including property and casualty reinsurance, life and health reinsurance, and specialty insurance solutions.	2

Table 1: Company Overview

The first group of interviewees included four professionals with extensive experience in governance consulting and auditing. Their backgrounds provided significant expertise in regulatory compliance, risk management, and governance frameworks, which are crucial for the effective management of IAM services. Insights from these experts were pivotal in understanding how IAM services are managed in relation to regulatory requirements and organizational standards. This group's input highlighted the complexities involved in ensuring IAM services adhere to compliance and governance expectations, thereby elucidating the broader implications for ITSM. The expertise offered by these professionals contributed to a detailed understanding of the distinct management practices required for IAM services, especially concerning regulatory adherence and risk management.

The second group comprised two professionals with specialized experience in IAM from a different organization. One of these individuals, a Product Owner, was responsible for overseeing the development and implementation of IAM solutions. This role provided detailed insights into the practical considerations involved in designing IAM services, including aspects such as user flexibility and modularity. The Product Owner's experience offered a perspective on how IAM services are structured to accommodate diverse user needs and the challenges associated with their implementation and management.

The other professional in this group, a Service Lead, managed IAM services for customers. This role encompassed operational aspects of IAM service delivery, such as scalability, resource management, and maintaining high performance standards. The Service Lead’s practical experience provided critical insights into the day-to-day challenges of managing IAM services, including strategies for handling varying demands and ensuring service reliability.

The combination of perspectives from these professionals, covering both governance and operational aspects, ensured a comprehensive exploration of IAM services. The diverse backgrounds and expertise of the interviewees contributed to a thorough analysis of the differences between IAM services and other IT services, as well as the specific implications for ITSM. This selection of interviewees facilitated a richer and more detailed analysis of IAM services, their distinct characteristics, and their impact on ITSM practices.

In summary, the choice of professionals from two different companies with varied expertise in governance consulting, auditing, and IAM management provided a multifaceted understanding of IAM services. This approach ensured a well-rounded examination of the topic, addressing both theoretical and practical dimensions of IAM and its implications for ITSM. The diverse perspectives contributed by the interviewees enhanced the depth and breadth of the research findings.

Reference	***Interview Number***	***Industrial Sector***	***Role***	***Years of Experience***
Interviewee I	1	Consulting / Audit	Senior Manager	10 Years
Interviewee II	2	Consulting / Audit	Director	11 Years
Interviewee III	3	Consulting / Audit	Manager	8 Years
Interviewee IV	4	Consulting / Audit	Consultant / Auditor	3 Years
Interviewee V	5	Insurance	CIAM Service Manager	3 Years
Interviewee VI	6	Insurance	CIAM Product Owner	3 Years

Table 2: Interviewee Overview

4.2 Design of Questionnaire

The design of the questionnaire for this thesis was meticulously crafted to address the assumptions related to IAM services and to explore their distinctive characteristics in comparison to other IT services. The questionnaire was structured to delve into the various dimensions outlined in the assumptions, thereby ensuring a thorough and nuanced understanding of the subject matter.

To address Assumption 1, which asserts that IAM services exhibit high user flexibility due to the frequent onboarding and offboarding of applications, the questionnaire incorporates questions designed to elicit comprehensive insights into how these processes are managed. For instance, questions such as "Can you provide detailed examples of how IAM services respond to frequent application onboarding and offboarding processes?" and "In what ways does the management of user identities in IAM services differ from that in other IT services?" are included. These questions are aimed at uncovering practical experiences and understanding the operational differences in identity management approaches. The goal is to capture how the dynamic nature of user and application management within IAM services influences their flexibility and adaptability.

Assumption 2 focuses on the scalability requirements inherent to IAM services, particularly the need for elastic resource allocation. To investigate this, the questionnaire includes targeted questions such as "What strategies and practices do you employ to ensure the scalability of IAM services?" and "How do you manage variable user loads, and what role does elastic resource allocation play in this context?" These questions are designed to explore the strategies and mechanisms used to effectively manage scalability and address variable user demands. Insights gathered from these questions aim to highlight the approaches and solutions employed to maintain optimal performance and resource allocation under varying conditions.

For Assumption 3, which emphasizes the criticality of IAM services and the necessity for effective availability management, the questionnaire poses questions intended to gather detailed information on these aspects. Questions such as "How do you define 'high effectiveness' in the context of availability management for IAM services?" and "What specific mechanisms and practices do you implement to ensure continuous service availability for IAM services?" are included. These inquiries seek to elucidate how availability and service continuity are managed within IAM services, focusing on the practices and strategies employed to maintain high service reliability and operational resilience.

To explore Assumption 4, which discusses the need for a modular service design in IAM services, the questionnaire features questions like "How is modularity incorporated into the service design of IAM services to address the diverse needs of customers?" and "Can you provide an example of how modularity in IAM services impacts service provision for both internal and external customers?" These questions are aimed at revealing how modular design principles are applied to meet the varied requirements of different user groups. The responses to these questions help to understand how modularity facilitates flexibility and customization in IAM services.

Finally, Assumption 5 addresses the integration of IAM services with other enterprise systems and highlights the importance of interoperability. To investigate this, the questionnaire includes questions such as "To what extent do IAM services require integration with other enterprise systems?" and "How do you prioritize and implement interoperability and standardized protocols in the context of IAM services?" These questions are designed to gather insights on the challenges and practices related to integrating IAM services with other systems. The aim is to explore how IAM services interact with broader IT infrastructures and the strategies used to ensure seamless integration and interoperability.

Although this thesis is written in English, it is noteworthy that most interviews were conducted in German. This approach was chosen to enable participants to articulate their experiences and insights more effectively in their native language. The transcripts of these interviews, along with the Interview Guide used during the sessions, are included in the appendix. The Interview Guide provides a detailed overview of the questions and structure of the interviews, offering additional context and clarification for understanding the responses and the research methodology. These resources collectively ensure a thorough and well-documented exploration of IAM services and their management, facilitating a comprehensive analysis of the research questions posed.

4.3 Data Collection

The qualitative data collection process for this research was meticulously designed and executed to ensure that the insights gathered would provide a profound understanding of the differences between IAM services and other IT services, as well as the implications of these differences for ITSM. This chapter outlines the comprehensive methods employed to gather data through interviews, which were central to addressing the research questions outlined in the preceding chapter.

The data collection process commenced with the development of a meticulously crafted interview guide. This guide was more than a mere compilation of questions; it was a carefully constructed instrument aimed at eliciting rich, descriptive narratives from the participants. The guide was designed to delve deeply into the specific characteristics of IAM services and their contrasts with other IT services. The inclusion of warm-up questions played a crucial role in this process. These initial questions were strategically formulated to ease the participants into the conversation, helping them to feel comfortable and open. This approach encouraged the interviewees to share their experiences candidly and facilitated a smoother transition into the core topics of discussion. The warm-up questions also helped to establish a context for the interview, guiding the conversation towards the nuances of IAM services and setting a foundation for exploring their implications for ITSM.

The interview guide, which is detailed in the appendix, ensured that each interview was conducted with a high degree of consistency and focus. This uniformity was essential for collecting comparable data across different sessions, allowing for a coherent analysis of the responses. The guide's structure was carefully designed to balance the need for consistency with the flexibility to explore emerging themes and insights during the interviews.

Ensuring the privacy and trust of the participants was a fundamental aspect of the research. A comprehensive privacy consent form was developed to outline the procedures for anonymizing data and the intended use of the collected information. This form was a critical element of the ethical framework of the study, providing participants with clear assurances regarding the confidentiality of their responses. The consent form outlined the measures taken to protect participants' identities and the steps involved in data handling. Each participant was required to review and sign this consent form before the interview commenced, thereby providing informed consent and reinforcing the ethical integrity of the research.

The interviews were conducted with a strong emphasis on respecting participants' privacy and comfort. Each session was audio-recorded to capture the full depth and nuance of the participants' responses. The use of audio recording was integral to ensuring the accuracy and reliability of the data collection process. These recordings served as a verbatim record of the interviews, which was essential for precise transcription and analysis.

Following the completion of the interviews, the transcription of the audio files was undertaken as a critical phase in the data handling process. Advanced transcription software was utilized to convert the spoken responses into written text. Each transcript was then meticulously reviewed to ensure accuracy and completeness. During this review process, any identifying information was carefully removed to maintain the anonymity of the participants. This step was crucial in safeguarding participant confidentiality and preparing the data for subsequent analysis.

Once transcribed, the data were organized into a comprehensive results matrix. This matrix served as an analytical tool that facilitated the systematic categorization and comparison of the interview data. It

provided a visual framework for identifying themes and patterns that emerged from the interviews, thus supporting a structured approach to qualitative analysis. The results matrix, which is presented in the appendix, became a foundational element for the thematic exploration discussed in the following chapter.

In conclusion, the qualitative interviews conducted for this research were a pivotal component in exploring the distinctions between IAM services and other IT services, as well as the implications of these differences for ITSM. The thorough preparation of the interview guide, the rigorous adherence to privacy and consent protocols, and the detailed transcription and anonymization of the data all contributed to the robustness and credibility of the research findings. The data collected through this meticulous process not only enhanced the understanding of the research topic but also provided a solid foundation for the analytical chapters that follow, ensuring a comprehensive exploration of IAM services within the context of ITSM.

5 Findings

In the initial analysis of responses to inquiries about the distinctive characteristics of IAM services compared to traditional IT services, a thematic consensus emerged among the participants. Interviewees I and III agreed that IAM services are primarily focused on mitigating organizational risks and ensuring compliance with regulatory requirements. Interviewee I elaborated that IAM services are unique due to their focus on the comprehensive lifecycle management of identities and access permissions. This view was supported by Interviewee VI, who emphasized the heightened centralization within IAM services, distinguishing them from other IT services that might adopt a more decentralized approach.

Interviewee II highlighted a different perspective, noting that IAM services are distinguished by their stronger emphasis on business integration. They argued that IAM encompasses components beyond traditional IT functions, thus integrating more deeply with business processes. Interviewee IV added another layer by pointing out the universal engagement of employees with IAM services across the company. According to Interviewee IV, the ideal IAM service should operate unobtrusively, integrating seamlessly into the work environment to maintain both security and user-friendliness without drawing undue attention.

The examination of Assumption 1 (A1), which posits that IAM services are distinguished by their high user flexibility due to frequent application onboarding and offboarding processes, revealed a range of responses that highlight the complexity of these services. The variation in responses reflects the diverse professional backgrounds of the interviewees. Those from the consulting sector emphasized process optimization and compliance, while interviewees from the insurance industry focused on operational challenges and practical implementation.

Interviewees I and VI underscored the significance of user numbers, particularly regarding onboarding. Interviewee I indicated that the performance of an IAM service is influenced by factors such as application size, user base, and technical integration. For example, Interviewee VI noted,

"*I would say that until now we federated customers to us with multiple email domains, because, you know, 10 to 15 email domains, and now we're working on 2,000s of email domains that we're federating, which you can scale it up to a number*" (Interviewee VI),

illustrating the substantial user flexibility due to onboarding processes. In the offboarding process, user accounts are deactivated or deleted after a specified period, completing the account lifecycle. These observations support A1 by demonstrating that IAM services offer greater flexibility compared to other applications, due to their capacity to dynamically and adaptively manage user integration.

Additionally, Interviewees V and VI emphasized that a significant focus of IAM services is on facilitating simple SSO integrations and developing automated onboarding and offboarding processes. This focus on user-centricity and process efficiency further substantiates the assumption of increased user flexibility.

The evaluation of Assumption 2, which asserts that the scalability of IAM systems due to variable user loads necessitates elastic resource allocation, showed a convergence in the perspectives of the inter-

viewees. Interviewees II and IV identified process automation as crucial for scalability, implying an increase in computational capacities. Interviewee I highlighted the critical role of load balancing for scalability, especially within Customer Identity and Access Management (CIAM) systems, where continuous permission verification leads to increased computational demands.

Interviewee VI advocated for the use of cloud services to achieve scalability, arguing that flexible resource allocation is necessary. He suggested that services should be decoupled and resources distributed to ensure optimal performance. Further discussions on Assumption 2 revealed that Interviewee III noted the complexity of control mechanisms as significantly impacting system performance, emphasizing the need for targeted planning during peak load times to ensure effective load balancing. Interviewee II supported this by stating,

"[…] these peaks must be managed through careful balancing and also by an appropriate allocation of system resources to effectively absorb these peaks, particularly to ensure usability for the end-users" (Interviewee II).

Interviewee IV stressed the importance of elastic resource allocation for authentication services, given that downtime can directly impact employee productivity. Although Interviewees I and II concurred that resource allocation might be of lower priority for internal IGA, Interviewee V highlighted the significance of cloud solutions and observability tools as proactive measures to ensure service continuity. Interviewee VI underscored the necessity of separating various IAM services and their environments to dynamically manage traffic and establish automated traffic distribution.

Resource usage within IAM systems can also be influenced by Segregation of Duties (SoD) requirements. Interviewee III provided an example, explaining that complex calculations associated with SoD methodologies can lead to higher and continuous computational demands. He stated,

"*For example, in the context of SoD, if I develop a methodology that requires very complex calculations, then I implement it once, and I may subsequently have a higher demand for computational power"* (Interviewee III).

In discussing how his organization handles variable user loads, he added,

"*I don't actually think there is a lot of variability in IAM. Where we do see fluctuations is in permission structures. The only points where variability can arise are when a new system is added or removed, but from my perspective, that's not significant enough to play with elastic resource allocation*"

(Interviewee III).

He further elaborated, "If there is a significant fluctuation in IAM, it can only result from two factors: either there is an organizational restructuring, like departments being relocated and tasks shifted, or there is a mistake or incident" (Interviewee III).

The assessment of Assumption 3, which contends that the critical nature of IAM services necessitates highly effective availability management with specific mechanisms to ensure service continuity, reaffirmed the critical importance of these services. Interviewees II and VI advocated for IAM Service-Level Agreements (SLAs) with nearly 100% availability due to the critical nature of these services. Interviewee IV provided a nuanced view, suggesting that while Identity Governance and Administration (IGA) within the IAM spectrum might require lower availability of 80-90%, PAM, which connects to other critical assets, demands higher availability, including for authentication services.

Interviewee II did not specify a particular availability figure but emphasized the importance of conducting a needs analysis to define high effectiveness in availability management based on organizational requirements and regulatory demands. Regarding mechanisms to ensure service continuity, Interviewees II, IV, V, and VI highlighted the importance of having Disaster Recovery plans to quickly restore services in the event of an outage. Interviewee V added that the use of observability tools can serve as a preventive measure, ideally preventing outages before they occur. Interviewee V also emphasized the importance of target systems having recovery plans to maintain continuity if the IAM service experiences downtime.

The investigation of Assumption 4, which contends that the diversity of subservices offered by IAM necessitates a modular service design to meet the varied needs of internal and external customers, elicited a range of opinions among experts. While some respondents, such as Interviewees V and VI, supported a broad array of services, Interviewees I, II, and III favored standardized solutions. Interviewee IV expressed concerns about modular offerings, cautioning,

"*If you construct a modular service portfolio and figuratively leave it to the customer to choose what they use, you will never achieve true centrality and uniformity across everything, as individuals will select what is easiest and perhaps cheapest for them*" (Interviewee IV).

This suggests that modularity may hinder centralization. Interviewee I echoed this concern, indicating that a modular approach might compromise adherence to regulatory requirements: "*I am actually not in favor of not deploying the full scope, as these processes have likely been defined for a reason, often by regulators such as BaFin, and are mandatory for the company to comply with*" (Interviewee I).

Nevertheless, Interviewees I and II agreed that a multitude of standard interfaces should be made available. Interviewee II elaborated,

"*If I have an SAP system, I need an SAP standard connector; for an Oracle system, an Oracle standard connector; for a PostgreSQL database, a PostgreSQL standard connector, to keep the onboarding hurdle as low as possible and thus ensure the broadest possible coverage of IAM across the organization's system landscape*" (Interviewee II).

This approach aims to achieve comprehensive coverage of the system landscape by reducing entry barriers through numerous standard connectors.

Interviewee II also addressed the impact of Customer Identity and Access Management (CIAM), noting,

Particularly with the focus on Customer Identity and Access Management, it has fundamentally altered the way customers interact with organization-specific services from the customer side. It has completely changed the customer's role in using the services that an organization offers in the B2C sector, as they are no longer just pure consumers of a service in terms of reading, using information provided by the organization in the B2C environment. Instead, they are effectively like the traditional internal enterprise user, an identity class that can actually make changes in the master data and customer master data themselves" (Interviewee II).

This shift enhances data accuracy but presents challenges in maintaining data integrity and centralization when integrating CIAM with other identity providers.

From an operational perspective, Interviewees V and VI argued for the importance of flexibility and modularity to address complex customer requirements. Interviewee V provided an example, stating,

"*A very good example here would be: We have a customer who is tackling risk assessments. They just want to make sure that the customer who is coming in has another layer of authentication. I mean,*

there's MFA, definitely, but they do a role-based authentication as well. And this role-based authentication is done on their system, which would mean that the style of the solution doesn't encompass what they need. Therefore, you see that this part, specifically the role-based access control that we have for the customers, usually differs based on the usage. You cannot really generalize. You cannot standardize in that way. You have to stay flexible" (Interviewee V).

Interviewee VI, as a Product Owner of a CIAM tool, added that their service provides the capability to customize alongside a standard set of services to cater to diverse customer needs.

The investigation of Assumption 5, which suggests that IAM services require a higher degree of integration with other enterprise systems compared to other IT services, affirmed the necessity for prioritizing interoperability and standardized protocols. Interviewee I highlighted the challenges posed by a heterogeneous system landscape for IAM solutions, stating,

"*We all know how diverse the technology world is, at least from an integration perspective, and this is naturally for IAM solutions as a central tool to which, in the best case, all applications should be connectable*" (Interviewee I).

This statement underscores the need for IAM solutions to integrate with diverse applications. Interviewee I also emphasized the importance of standard connectors for integrating key or standardized software solutions, such as ERP systems or Active Directories, into IAM services.

Interviewee II added that standards are crucial for simplifying the enforcement of controls and minimizing the risk of data integrity loss. This means that a higher degree of standardization and integration also enhances the effectiveness of controls. Interviewees II, III, IV, and V supported the importance of integration, with Interviewees IV and V advocating for compliance with industry standards. Interviewee III reinforced the necessity of standards for easy integration, advising,

"*And if necessary, do not purchase software that cannot handle these standard protocols*" (Interviewee III).

Despite the emphasis on standards and integration, it is evident that achieving a balance between flexibility, modularity, and standardization is crucial for the effective management and implementation of IAM services.

6 Conclusion

In response to the first research question, which sought to identify the distinct characteristics of IAM services compared to other IT services, the analysis revealed several defining features that set IAM apart. These characteristics not only highlight the unique aspects of IAM but also illuminate how these services diverge fundamentally from other IT functions within an organization.

A primary distinguishing characteristic of IAM services is their exceptional user flexibility. This flexibility arises from the frequent onboarding and offboarding of users, which is integral to the operation of IAM systems. Unlike many IT services that might deal with more static user populations, IAM services are tasked with dynamically managing the lifecycle of user accounts. This includes handling the creation, modification, and deletion of user identities in response to organizational changes. The ability of IAM services to adapt rapidly to fluctuations in user numbers and to accommodate a diverse array of application scenarios underscores their unique role. This dynamic management capability ensures that IAM services can efficiently handle the continuous flow of user access requests and changes, which is a distinct feature compared to other IT services that may not require such frequent adjustments.

Another significant feature of IAM services is their modular service design, which is crucial for supporting a broad range of subservices. IAM solutions often include various components such as authentication mechanisms, access control systems, and identity governance tools. The modular nature of these services allows for a tailored approach to meet the specific needs of both internal users and external clients. While modularity introduces complexity, particularly concerning centralization and regulatory compliance, it remains essential for adapting IAM services to a heterogeneous IT environment. The modular approach enables IAM services to integrate effectively with different systems and applications, providing flexibility in how they are deployed and managed within the organization.

Furthermore, IAM services are distinguished by their high level of integration with other enterprise systems. Given their central role in managing user access and ensuring security, IAM services must operate seamlessly with a wide range of applications and IT infrastructure components. This necessitates the use of standardized protocols and interfaces to ensure interoperability. Unlike other IT services that might operate independently or with less frequent integration demands, IAM services require a cohesive approach to integration. Effective interaction with various systems is critical for maintaining the overall integrity and security of the IT environment. This integration capability highlights how IAM services must be embedded within the broader IT landscape to function optimally.

Addressing the second research question, which explored the implications of these distinct characteristics for IT Service Management, several key points emerged. The scalability requirements of IAM services, driven by variable user loads and the need for flexible resource allocation, have significant implications for ITSM. Effective management of IAM services necessitates ITSM practices that can adapt to changes in user demand and system performance. The interviews underscored the importance of implementing process automation, load balancing, and cloud-based solutions to manage these demands effectively. ITSM strategies must be designed to accommodate dynamic resource needs and ensure that IAM services can scale appropriately during periods of high demand, maintaining performance and availability.

Moreover, the critical role of IAM services in ensuring secure access and operational continuity underscores the need for robust availability management within ITSM. The requirement for near-constant availability of certain IAM components, such as Privileged Access Management (PAM) systems and authentication services, was a key finding. To address this, ITSM practices must include comprehensive disaster recovery plans and advanced observability tools. These measures are essential for preventing service disruptions and maintaining the reliability of IAM services. The focus on availability highlights the need for ITSM approaches that prioritize the uninterrupted operation of critical IAM components to support overall business continuity.

Finally, the high degree of integration required by IAM services suggests that ITSM must prioritize interoperability and the adoption of standardized protocols. Ensuring effective control enforcement and maintaining data integrity across a diverse technological landscape depends on seamless integration of IAM solutions with other IT systems. ITSM strategies must be crafted to support these integration needs, ensuring that IAM services function as integral, reliable elements within the organization's IT infrastructure. This involves adopting and adhering to standardized interfaces and communication protocols that facilitate smooth and secure interactions between IAM systems and other enterprise applications.

In conclusion, the unique characteristics of IAM services, such as their high user flexibility, modular design, extensive integration needs, and critical role in security and operational continuity, highlight their distinct nature compared to other IT services. These features necessitate specialized ITSM approaches that focus on scalability, availability, and integration. The findings provide a detailed understanding of how IAM services differ from other IT functions and outline the specific management strategies required to optimize their deployment and operation within an organization. By addressing these unique aspects, organizations can better manage their IAM services and ensure their effective integration into the broader IT ecosystem.

To build on the analysis, it is crucial for IT service managers to emphasize a clear scope definition when managing IAM services. Given the inherent flexibility and variability of these services, defining their scope is more complex than with other IT services. IAM services involve frequent user onboarding and offboarding, extensive integration with enterprise systems, and dynamically shifting access needs. As a result, poorly defined scopes can lead to inefficiencies, misaligned resource allocation, and potential security risks. A well-defined scope ensures that the boundaries of the IAM service are clear, making it easier to manage its modular components and the integration with other systems. This clarity is especially important given the fluctuating user volumes and the need for seamless interoperability with a variety of IT platforms. By focusing on scope during service definition, IT managers can prevent operational disruptions and ensure that the IAM service supports the organization's evolving requirements effectively. In addition to emphasizing the importance of scope definition, IT service managers should also focus on continuous alignment with business objectives. As IAM services are highly dynamic and integral to security and compliance, maintaining close collaboration with other business units is crucial. Regularly revisiting the scope and adapting it as organizational needs evolve can help avoid misalignments between the service provided and the business goals. Moreover, IT service managers should consider investing in automation and monitoring tools to manage the scalability and integration complexities of IAM services efficiently, ensuring both operational resilience and security.

By aligning IAM service management with these strategic considerations, IT service managers can better navigate the complexities of IAM systems and ensure they are optimally managed within the broader IT ecosystem. These recommendations are crucial for ensuring that IAM services not only meet technical requirements but also contribute to the broader goals of organizational security and operational efficiency. Such an approach helps mitigate risks, enhances service reliability, and supports the sustainable growth of the IT infrastructure in an increasingly interconnected environment.

Reflecting on these conclusions, the diagram that visually represents the relationship between IAM characteristics and ITSM focus areas has been updated. The revised diagram now includes key elements such as Centralized User Management and additional factors that emphasize the evolving nature of IAM services and their implications for ITSM. This updated diagram, which is presented below, integrates the new insights and recommendations derived from the research and offers a clearer visual representation of how IAM characteristics map to ITSM practices.

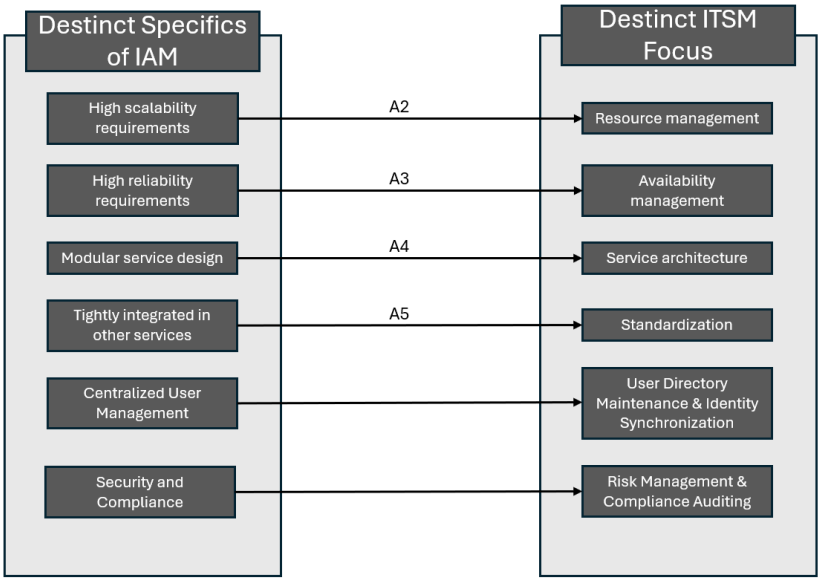

Figure 5 Update Research Diagram

The revised diagram includes two new connections that enhance the depiction of how IAM characteristics influence ITSM practices:

Centralized User Management is now linked to User Directory Maintenance & Identity Synchronization. Centralized user management in IAM systems focuses on the streamlined administration of user identities across multiple platforms. This characteristic has direct implications for ITSM, particularly in maintaining accurate user directories and ensuring identity synchronization. By emphasizing this link, the diagram highlights the importance of effective ITSM practices in supporting the seamless operation of centralized IAM functions and ensuring that user data is consistently updated and aligned with organizational changes.

Security and Compliance is connected to Risk Management & Compliance Auditing. IAM services play a critical role in managing security and meeting compliance requirements. This characteristic influences ITSM's approach to risk management and compliance auditing. The diagram now underscores the need for ITSM strategies to address the security and compliance demands of IAM systems. This connection emphasizes the importance of integrating risk management and compliance auditing into ITSM practices to ensure robust security measures and regulatory adherence.

These additions provide a more nuanced view of the interplay between IAM characteristics and ITSM focus areas, offering a comprehensive perspective on how specific IAM attributes drive targeted ITSM practices.

7 Discussion

7.1 Limitation

In conducting this research on IAM services and their implications for ITSM, several limitations must be acknowledged. These limitations arise from the study's methodological choices, scope, and focus, which shape the overall findings and their applicability.

Firstly, the research adopted a deductive approach, which was designed to test specific assumptions derived from existing literature and theoretical frameworks. This approach provided a structured means to evaluate predefined assumptions about IAM services. However, the deductive nature of the research inherently constrained the exploration of broader aspects of ITSM that could be influenced by IAM services. By focusing on particular assumptions, the study may have missed out on discovering new, unanticipated relationships between IAM and ITSM processes. This limitation implies that while the study offers valuable insights into specific assumptions, it does not fully capture the complexity of how IAM services might interact with ITSM in a more expansive or holistic manner.

Secondly, the research concentrated on certain areas within ITSM that were identified as most relevant based on the initial assumptions. This selective focus allowed for a detailed examination of particular aspects of IAM's impact, such as user flexibility and scalability. However, this focus excluded other potentially significant domains within ITSM, such as Incident Management, Problem Management, Change Management, Service Request Management, and Service Level Management. These areas are integral to ITSM and could be significantly impacted by IAM services. By not exploring these domains in detail, the study may have provided an incomplete picture of IAM's influence on the broader ITSM landscape. Consequently, the findings may not fully reflect the range of ways in which IAM services affect different ITSM processes and practices.

Additionally, the research relied heavily on qualitative data collected from a relatively small number of interviews. Although these interviews provided rich and detailed insights, the limited sample size and specific selection of interviewees may have introduced bias into the findings. The perspectives gathered were from a select group of professionals, which might not represent the broader ITSM community or the diversity of IAM implementations across various industries. Different organizations may have unique experiences and challenges related to IAM that were not captured in this study. The limited diversity in the sample could affect the generalizability of the findings, making it difficult to apply the results universally across different contexts and organizational settings.

Moreover, the study's emphasis on particular characteristics of IAM services, such as user flexibility, scalability, and integration, might have overshadowed other critical dimensions of IAM management. For example, aspects such as security, user experience, and regulatory compliance are crucial to the effective implementation and management of IAM services within ITSM frameworks. By focusing primarily on specific characteristics, the study may have neglected these important factors, which could also play a significant role in shaping the interaction between IAM and ITSM processes. This limited focus means that the findings may not provide a comprehensive view of all the relevant aspects of IAM services and their impact on ITSM.

Another important consideration is the temporal and contextual scope of the study. The research was conducted within a specific timeframe and focused on the perspectives of professionals based on the current state of IAM and ITSM practices. Given the rapidly evolving nature of technology and organizational practices, the findings may quickly become outdated or less relevant as new developments emerge. The dynamic nature of ITSM and IAM means that ongoing changes in technology, regulations,

and organizational needs could influence the applicability and relevance of the study's conclusions over time.

Furthermore, the study's findings are also limited by the potential variability in how IAM services are implemented and managed across different organizations. The study may not account for variations in IAM practices, tools, and technologies used by different organizations, which could affect how IAM interacts with ITSM processes. Variations in implementation strategies, organizational structures, and IT environments could lead to different outcomes and experiences that were not captured in this research. This variability further limits the ability to generalize the findings to all organizational contexts.

In summary, while this research provides valuable insights into specific aspects of IAM services and their implications for ITSM, it is crucial to acknowledge the limitations arising from the deductive approach, selective focus on certain ITSM domains, reliance on a limited sample size, emphasis on specific IAM characteristics, and the dynamic nature of technology and organizational practices. These limitations should be considered when interpreting the study's findings and understanding their scope. Recognizing these constraints helps to frame the results within their appropriate context and highlights areas where further research could provide a more comprehensive understanding of IAM's role in ITSM.

7.2 Future Work

Considering the limitations identified in this study, future research on IAM and its implications for ITSM-presents several promising directions that could further enrich our understanding of these critical areas. To build on the insights garnered from this research, it is essential to consider employing both quantitative and inductive approaches. Each of these methodologies offers unique advantages that could contribute to a more comprehensive and nuanced understanding of IAM’s distinctive characteristics and their broader impact on ITSM.

A significant opportunity for future research lies in adopting a quantitative approach. This method involves the systematic collection and analysis of numerical data from a diverse range of organizations. By performing statistical tests on this data, researchers can evaluate and validate the assumptions proposed in this study. For instance, gathering data on metrics such as the frequency and impact of IAM-related incidents would allow researchers to quantify how often these incidents occur and their effect on ITSM processes. Such analysis could provide empirical support for the qualitative insights presented in this thesis and help generalize findings across various industries and organizational settings.

Furthermore, quantitative research could focus on key performance indicators related to scalability and performance. By examining how IAM systems handle varying loads and the effectiveness of their integration protocols, researchers can offer concrete evidence on the operational efficiency of IAM services. Metrics such as system responsiveness during peak times, the accuracy of user access management, and the efficiency of integration with existing ITSM frameworks are critical for understanding IAM’s impact. Exploring these aspects through quantitative analysis would provide a clearer picture of how IAM systems influence ITSM practices and highlight areas for potential improvement.

Additionally, quantitative research could investigate correlations between IAM implementations and measurable outcomes in ITSM. For example, analyzing the relationship between IAM practices and service availability, incident response times, or compliance with regulatory standards could offer valuable insights. Understanding these correlations would not only validate the findings of this study but also help organizations optimize their IAM strategies to achieve better alignment with ITSM best practices.

In conjunction with quantitative methods, an inductive approach offers a complementary avenue for future research. This approach emphasizes exploratory investigation and allows researchers to identify new areas of influence that may not be apparent through hypothesis/assumption-driven studies. By examining real-world implementations of IAM services and observing emerging patterns and trends, researchers can uncover additional domains within ITSM that are affected by IAM but were not initially considered.

For instance, inductive research could reveal new insights into how IAM interacts with ITSM processes such as change management, incident management, and service level management. By starting with detailed observations and patterns, researchers can identify previously overlooked aspects of IAM's impact. This approach allows for a more open-ended exploration of IAM's role, providing a broader understanding of how IAM services affect various ITSM functions and potentially uncovering new areas of influence.

Combining quantitative and inductive approaches in future research could provide a more holistic and in-depth view of IAM's impact on ITSM. While quantitative methods offer empirical support and generalizability, inductive research ensures that no significant areas of influence are missed. Together, these approaches would contribute to a richer and more comprehensive understanding of how IAM services interact with ITSM practices. This integrated methodology would not only validate and extend existing knowledge but also offer specific, actionable recommendations for practitioners.

In summary, future research should focus on incorporating quantitative methods to strengthen the empirical foundation of IAM studies and employing inductive methods to explore new areas of influence. By leveraging these approaches, researchers can build on the findings of this thesis and contribute to a deeper and more nuanced understanding of IAM's role in IT Service Management. Such efforts will provide valuable insights for both academic scholars and industry practitioners, guiding the optimization of IAM strategies and the enhancement of ITSM practices. The integration of quantitative data with exploratory research will ensure a comprehensive examination of IAM's impact, ultimately leading to more effective and aligned ITSM practices.

References

Axelos. (2019). ITIL foundation: ITIL 4 edition.

Axelos. (2021). ITIL 4: Direct, plan and improve.

Galup, S. D., Dattero, R., Quan, J. J., & Conger, S. (2009). An overview of IT service management. Communications of the ACM, 52(5), 124-128. https://doi.org/10.1145/1506409.1506439

Hochstein, A., Tamm, G., & Brenner, W. (2005). Service-oriented IT management: Benefit, cost and success factors. In Proceedings of the European Conference on Information Systems (ECIS).

IT Governance Institute. (2007). COBIT 4.1. ITGI.

Marrone, M., & Kolbe, L. M. (2011). Impact of IT service management frameworks on the IT organization. Business & Information Systems Engineering, 3(1), 5-18. https://doi.org/10.1007/s12599-010-0141-5

Office of Government Commerce. (2007). The official introduction to the ITIL service lifecycle.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

Kavis, M. J. (2014). Architecting the cloud: Design decisions for cloud computing service models (SaaS, PaaS, and IaaS). John Wiley & Sons.

Marinescu, D. C. (2017). Cloud computing: Theory and practice. Morgan Kaufmann.

Doerbecker, R., & Boehmann, T. (2013). The concept and effects of service modularity – A literature review. In Proceedings of the 46th Hawaii International Conference on System Sciences (pp. 1357-1366). IEEE.

Bertino, E., & Takahashi, K. (2010). Identity management: Concepts, technologies, and systems. Artech House.

Ferraiolo, D. F., & Kuhn, D. R. (1995). Role-based access controls. Proceedings of the 15th NIST-NCSC National Computer Security Conference, 554-563.

ISO/IEC 27001. (2013). Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization.

National Institute of Standards and Technology (NIST). (2019). Digital identity guidelines (NIST Special Publication 800-63-3). https://doi.org/10.6028/NIST.SP.800-63-3

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12), 2021-2040. https://doi.org/10.1109/JPROC.2003.819611

Tep, K. S., Martini, B., Hunt, R., & Choo, K.-K. R. (2015). A taxonomy of cloud attack consequences and mitigation strategies: The role of access control and privileged access management. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, 926-933. IEEE. https://doi.org/10.1109/Trustcom.2015.485

Jostein, J. (2012). Federated identity management challenges. In Proceedings of the 7th International Conference on Availability, Reliability, and Security (ARES 2012), 230-237. IEEE.

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing (NIST Special Publication 800-144). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-144

National Institute of Standards and Technology (NIST). (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53, Revision 5). https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). https://doi.org/10.6028/NIST.CSWP.04162018

Kobelsky, K. W. (2014). A conceptual model for segregation of duties: Integrating theory and practice for manual and IT-supported processes. International Journal of Accounting Information Systems

Glazer, I. (2023). Introduction to Customer Identity and Access Management. IDPro Body of Knowledge, 1(12).

Bryman, A. (2016). Social research methods. Oxford university press.

Appendix

Appendix 1: Interview Guide

General Data:

Interview-Typ	**[TYP]**
Interview-Number	**[Number]**
Interview Date	**[DD.MM.YYYY]**
Interview-Duration (in Minuten)	**[Time]**

Demographic Data:

Industrial Sector	**[Sector]**
Role	**[Role]**
Experience in IAM / ITSM (in Years)	**[Years]**

English Version

Introduction words:

Thank you for taking the time to conduct an interview with me as an expert today. Before we start the interview, I would like to briefly introduce myself and give you some information about me. My name is Manuel Yambao and I am in the final stages of my Business Information Technology bachelor's degree at the University for applied Science Ulm and University for applied Science Neu-Ulm.

As part of the interview, I would like to ask you some questions regarding ITSM and IAM services. If you agree to this, please confirm briefly. If you have no questions, I would now like to start the interview. Otherwise, we can clarify any open questions you may have beforehand.

Warm-up-Question:

At the beginning of the interview, please tell me about the general tasks you perform in your company.

What characteristics does an IAM service have that distinguishes it from other IT services?

Main Questions:

Can you provide examples of how IAM services respond to frequent application onboarding and off-boarding processes?

How does the management of user identities in IAM services differ from that in other IT ser-vices?

What strategies do you employ to ensure the scalability of IAM services?

How do you handle variable user loads, and what role does elastic resource allocation play in this con-text?

How do you define 'high effectiveness' in the context of availability management for IAM services?

What specific mechanisms do you implement to ensure service continuity for IAM services?

How is modularity implemented in the service design of IAM services to meet the diverse needs of customers?

Can you give an example of how modularity in IAM services affects service provision for internal and external customers?"

To what extent do IAM services require a higher level of integration with other enterprise systems?

How do you prioritize interoperability and standardized protocols in the context of IAM services?

Interview Closure:

Are there any points from your side that have not yet been addressed but that you would like to add?

Final Words:

I sincerely thank you for your willingness and time you have taken to conduct an interview with me. Should you be interested in the results of my bachelor's thesis, I will approach you in September and present them to you.

German Version

Einleitungsworte:

Vielen Dank, dass Sie sich heute die Zeit nehmen, ein Interview mit mir als Experten zu führen. Bevor wir mit dem Interview beginnen, möchte ich mich kurz vorstellen und Ihnen einige Informationen über mich geben. Mein Name ist Manuel Yambao und ich befinde mich in der Endphase meines Bachelorstudiums der Wirtschaftsinformatik an der Hochschule Ulm und der Hochschule Neu-Ulm. Im Rahmen des Interviews möchte ich Ihnen einige Fragen zu ITSM- und IAM-Diensten stellen. Wenn Sie damit einverstanden sind, bestätigen Sie bitte kurz. Wenn Sie keine Fragen haben, würde ich jetzt gerne mit dem Interview beginnen. Andernfalls können wir vorher etwaige offene Fragen klären.

Aufwärmfrage: Erzählen Sie mir bitte zu Beginn des Interviews von den allgemeinen Aufgaben, die Sie in Ihrem Unternehmen ausführen.

Welche Merkmale hat ein IAM-Service, der ihn von anderen IT-Services unterscheidet?

Hauptfragen:

Können Sie Beispiele dafür geben, wie IAM-Services auf häufige Applikations On- und -Offboardingprozesse reagieren?

Wie unterscheidet sich die Verwaltung von Usern in IAM-Services von der in anderen IT-Services?

Welche Strategien würden Sie einsetzen, um die Skalierbarkeit von IAM-Diensten zu gewährleisten?

Wie gehen Sie mit variablen Userlasten um und welche Rolle spielt die flexible Ressourcenzuweisung in diesem Zusammenhang?

Wie definieren Sie 'hohe Effektivität im Kontext des Availabilitymanagement für IAM-Services?

Welche spezifischen Mechanismen würden Sie einsetzen, um die Kontinuität für IAM-Services zu gewährleisten?

Wie wird Modularität im Servicedesign von IAM-Diensten implementiert, um den vielfältigen Bedürfnissen der Kunden gerecht zu werden?

Können Sie ein Beispiel dafür geben, wie Modularität in IAM-Services die Dienstleistung für interne und externe Kunden beeinflusst?

Inwieweit erfordern IAM-Services eine höhere Integrationsebene mit anderen Unternehmenssystemen?

Wie priorisieren Sie Interoperabilität und standardisierte Protokolle im Kontext von IAM-Services?

Interviewabschluss: Gibt es von Ihrer Seite aus Punkte, die noch nicht angesprochen wurden, die Sie aber hinzufügen möchten?

Schlussworte:

Ich danke Ihnen aufrichtig für Ihre Bereitschaft und die Zeit, die Sie sich genommen haben, um ein Interview mit mir zu führen. Sollten Sie an den Ergebnissen meiner Bachelorarbeit interessiert sein, werde ich Sie im September darauf ansprechen und sie Ihnen präsentieren.

Appendix 2: Literature Paper Review

1	**Identity management distilled, a comparison of frameworks** **Authors: Pieter Wisse, Paul Jansen**
2	**Identity and access management in cloud environment: Mechanisms and challenges** **Authors: I. Indu, P.M. Rubesh Anand, Vidhyacharan Bhaskar**
3	**Intelligent authentication for identity and access management: a review paper** **Authors: Ishaq Azhar Mohammed**
4	**Economics of Identity and Access Management: Providing Decision Support for Investments** **Authors: Ishaq Azhar Mohammed**
5	**Identity and Access Management as Security-as-a-Service from Clouds** **Authors: Deepak H. Sharmaa, Dr. C. A. Dhoteb, Manish M. Poteyc**
6	**Identity and Access Management System: a WebBased Approach for an Enterpris** **Authors: Ishaq Azhar Mohammed**
7	**Systematic Review of Identity Access Management in Infomation Security** **Authors: Ishaq Azhar Mohammed**
8	**Blockchain-based identity management systems: A review** **Authors: Yang Liu a, Debiao He , Mohammad S. Obaidat, Neeraj Kumarf ,Muhammad Khurram Khan , Kim-Kwang Raymond Choo**
9	**Federated Identity Management** **Authors: Simon S.Y. Shim, Geetanjali Bhalla, Vishnu Pendyala**
10	**User Centric Identity Management** **Authors: Audun Jøsang, Simon Pope**
11	**IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations** **Authors: Chetanpal Singh, Jatinder Warraich, Rahul Thakkar**
12	**Optimizing Identity and Access Management** **Authors: Ali M. Al-Khouri**
13	**An Integrated Approach for Identity and Access Management in a SOA Context** **Authors: Waldemar Hummer, Patrick Gaubatz, Mark Strembeck, Uwe Zdun, Schahram Dustdar**

14	**A Survey of Identity Management Technology** **Authors: Yuan Cao, Lin Yang**
15	**Attribute quality management for dynamic identity and access management** **Authors: Michael Kunz a, Alexander Puchta, Sebastian Groll , Ludwig Fuchs , Günther Pernul**
16	**Integrated identity and auditing management using blockchain mechanism** **Authors: Prashant Madhukar Yawalkar, Deepak Narayan Paithankar, Abhijeet Rajendra Pabale, Rushikesh Vilas Kolhe , P. William**
17	**Trust Requirements in Identity Management** **Authors: Audun Jøsang, John Fabre, Brian Hay, James Dalziel, Simon Pope**
18	**Consider Identity and Access Management as a Process, Not a Technology** **Authors: Earl L. Perkins, Ant Allan**
19	**Proposed Identity and Access Managementin Future Internet (IAMFI): A BehavioralModeling Approach** **Authors: Nancy Ambritta P., Poonam N. Railkar and Parikshit N. Mahalle**
20	**Federated Identity Management Challenges** **Authors: Jostein Jensen**

Appendix 3: Interview Transcript I

General Data:

Interview-Type	**MS-Teams**
Interview-Number	**1**
Interview Date	**25.07.2024**
Interview-Duration (in Minutes)	**29min**

Demographic Data:

Industrial Sector	**Consulting**
Role	**Senior Manager**
Experience in IAM / ITSM (in Years)	**10 Jahre**

I: Vielen Dank, dass Sie sich heute die Zeit nehmen, ein Interview mit mir als Experten zu führen. Bevor wir mit dem Interview beginnen, möchte ich mich kurz vorstellen und Ihnen einige Informationen über mich geben. Mein Name ist Manuel Yambao und ich befinde mich in der Endphase meines Bachelorstudiums der Wirtschaftsinformatik an der Hochschule Ulm und der Hochschule Neu-Ulm. Im Rahmen des Interviews möchte ich Ihnen einige Fragen zu ITSM- und IAM-Diensten stellen. Wenn Sie damit einverstanden sind, bestätigen Sie bitte kurz. Wenn Sie keine Fragen haben, würde ich jetzt gerne mit dem Interview beginnen. Andernfalls können wir vorher etwaige offene Fragen klären.

I: Erzählen Sie mir bitte zu Beginn des Interviews von den allgemeinen Aufgaben, die Sie in Ihrem Unternehmen ausführen.

A: Als Senior Manager bei den Big Four zählen zu meinen Kernaufgaben natürlich Projekte zu managen, also als Engagementmanager unterwegs zu sein, das heißt, angefangen von Projekte gewinnen, sprich, bei den Kunden Pitches mitzumachen, Angebote zu erstellen, aber dann über das Delivery, sprich dafür zu sorgen, dass das richtig richtige Team zusammengestellt wird, dass die Aufgaben klar verteilt werden, für den Aufbau des Teams und Ausbildung des Teams zu sorgen, aber auch für die Qualität der gelieferten Leistungen dann entsprechend zu sorgen.

I: Welche Merkmale hat ein IAM-Service, der ihn von anderen IT-Services unterscheidet?

A: Ich würde es folgendermaßen beantworten: Ich würde behaupten, dass im auch ein IT Service ist. Das heißt, ITSM steht aus meiner Sicht oben drüber weil IAM an sich ist ja auch eine IT-Dienstleistung oder IT Tool ist, die den Service unterstützt und aus technischer Sicht gelten da ja ähnliche Anforderungen und Vorgaben die für jeden anderen IT Service gelten, sei es Verfügbarkeit, sei es Tickets wenn die Software nicht läuft, über ITSM dessen Prozesse entsprechend steuern, was aber hier IAM spezifisch ist, sind glaube ich die Ziele der Software oder der Lösung an sich, weil da geht es ja darum die Identitäten und Berechtigung entsprechend entlang des gesamten Lebenszyklus zu begleiten. Ich würde mal sagen, dass die technische Seite einer IAM Lösung die gehört oder wird vom ITSM entsprechend mit abgedeckt werden aber die Logik von IAM Lösung, die sind tatsächlich separat zu betrachten.

I: Können Sie Beispiele dafür geben, wie IAM-Services auf häufige Applikations On- und -Offboardingprozesse reagieren?

A: Performance technisch mit Sicherheit wobei, das hängt dann meistens auch davon ab, wie groß die Anwendung, die gerade angebunden wird, dann an sich ist, beziehungsweise wie groß der Nutzerkreis der Anwendung ist. Weil das schon dann ein Unterschied macht, ob ich ein SAP System an eine bestehende Lösung anbinde oder eine Anwendung bei vielleicht nur zwei User drauf sind. Da ist entsprechend auch die Last die auf IAM dann ankommt unterschiedlich. Die entscheidende Frage ist aber aus meiner Sicht auch die Art der Anbindung an das IAM, denn es gibt im Fach-Jargon sogenannte Bi-Direktionale-Schnittstellen oder auch nur lesende Schnittstellen, und das hat natürlich ganz große Auswirkungen darauf, wie sich das auf die Performance der Software auswirkt. Das heißt, wenn ich die IAM Lösung übertrieben gesagt nur als ein Beantragungstool, als Workflow nutze und dann gar keine richtige Schnittstelle Richtung Anwendung brauche, dann ist natürlich die Auslastung bzw. die Belastung der Software an sich auch nicht so stark. Zusätzlich kommt noch der Punkt zum Tragen, ob es immer eine live Überprüfung der Berechnung erfolgt, sprich die Performance von IAM immer beansprucht wird oder wird die Berechnung einmal eingerichtet und dann gibt es keine Kommunikation mehr dazwischen, bis dann irgendwann unter gewissen Umständen oder Abständen die Daten abgeglichen werden.

I: Wie unterscheidet sich die Verwaltung von Usern in IAM-Services von der in anderen IT-Services?

A: Ich glaub hier wiederum ist dann ein IAM Tool oder ein Idm Tool quasi führend und würde auch über allen anderen Services drüber stehen. Ähnlich wie ich generell ITSM zu IAM beschrieben habe, gilt es genauso, wenn es um die Identitätsverwaltung geht. Da übernimmt dann aus meiner Sicht das IAM-Tool.

I: Welche Strategien würden Sie einsetzen, um die Skalierbarkeit von IAM-Diensten zu gewährleisten?

A: Richtig skalieren kann man es wahrscheinlich nur durch Performance, also genug Performance zu haben durch Verteilung der Last. Also klassische Themen wie Load-Balancing und so weiter wobei da muss man fairerweise sagen, das IAM ist jetzt kein Tool ist wo 20 000 User gleichzeitig darauf zugreifen, außer wie gesagt die Sonderfälle, die ich anfangs auch schon angesprochen habe. Es gibt gewisse Lösungsansätze, wo diese Berechtigungsprüfung in Echtzeit überprüft wird. Da ist es natürlich ein bisschen anspruchsvoller, aber im Normalfall hast du ja keine ständige Interaktion zwischen dem User oder

der Applikation und dem IAM-Tool, deswegen ist es nicht ganz anwendbar, anders ist es aber tatsächlich, was seit Jahren ja, jetzt immer mehr eingesetzt wird, sind sogenannte Customer Identity and Access Management Tools, die beispielsweise bei den Banken oder Onlineshops oder solchen Unternehmen eingesetzt werden, wo tatsächlich ganz viele User gleichzeitig auch die Software zugreifen wollen oder auf Webshop, sei es Amazon oder ähnliche Themen. Da ist es natürlich wichtig, weil da werden die Rechte auch immer sobald du die Seite aufgemacht hast, überprüft und dann ist natürlich die Last auf die Server deutlich größer, im Vergleich wie sie in einem klassischen Unternehmen sein wird.

I: Wie gehen Sie mit variablen Userlasten um und welche Rolle spielt die flexible Ressourcenzuweisung in diesem Zusammenhang?

A: Wie eben angesprochen, in einem klassischen Unternehmen spielt es aus meiner Sicht keine wesentliche Rolle, weil die Anfragen einfach nicht so oft vorkommen. Es gibt auch vermehrt oder jetzt immer öfter die Ansätze des sogenannten Rollbase Access Management, wo es darum geht, dass die Rollen nicht einzeln beantragt werden oder die Berechnung auf einzelne Applikationen, sondern man sogenannte Business rollen baut, welche dann alle Zugriffe, die ein Mitarbeiter für seine Tätigkeit benötigen zusammenfasst. Das bedeutet dann auch am Ende des Tages, dass du einen Antrag stellst, die Rechte einmal zugewiesen werden und dann gibt es keine Interaktion mehr. Deswegen ist diese echte Last ist eigentlich nicht da, mit Ausnahmen, die ich eben auch schon besprochen habe. Nichtsdestotrotz gibt es natürlich einige kritische Applikationen, wo es gewährleistet soll, dass die Rechte schnell zugewiesen werden, wenn wir an Themen wie Sicherheitskontrollen oder sowas denken, also bei Zutritt auf ein Gelände oder so, da muss natürlich sichergestellt werden, dass die Rechte schnell zugewiesen werden, das heißt, da ist trotzdem die Anforderung da, natürlich die Verfügbarkeit zu haben ob unterschiedliche Unternehmen hier jetzt die Cloud Service oder eigene Serverräume immer noch nutzen, sorgen natürlich dafür, dass da entsprechende, Verfügbarkeit gegeben ist.

I: Wie definieren Sie 'hohe Effektivität im Kontext des Availabilitymanagement für IAM-Services?

A: Das ist interessante Frage. Jeder User will schnell an seine Rechte rankommen, sprich Antrag abschicken und im Best Case hast du in der gleichen Sekunde dein Recht bekommen, in Wirklichkeit sieht es aber tatsächlich so aus, dass es zu Verzögerung kommen kann und dafür sprechen ja unterschiedlichste Gründe, sei es der Genehmigungsworkflow an sich, also sprich beispielsweise beim Vorgesetzten, wie schnell er das Ticket überhaupt bearbeitet und eine Genehmigung gegeben hat. Schwer zu definieren. Da gibt es keine richtige Lösung, jedes Unternehmen definiert es für sich und vor allem eine mit einer Einstufung von Kritikalität der Applikation. Im Zweifel gibt es dann für jede kritische Anwendung auch Notlösungen im Sinne von manueller Provisionierung, die man bei Bedarf dann auch noch durchführen könnte.

I: Welche spezifischen Mechanismen würden Sie einsetzen, um die Kontinuität für IAM-Services zu gewährleisten?

A: [Keine Antwort]

I: Wie wird Modularität im Servicedesign von IAM-Diensten implementiert, um den vielfältigen Bedürfnissen der Kunden gerecht zu werden?

A: Aktuellen gibt es ja schon recht viele unterschiedliche Anbieter für IAM. Das ist in der Tat so, dass je nachdem wie groß das Unternehmen an sich ist oder also der Kunde an der Stelle greift, man dann meistens auch auf unterschiedliche Anbieter auch zu. Insbesondere für die kleinere Unternehmen gibt es viele Cloud Anbieter, die recht pragmatische und einfache Lösungen gebaut haben. Es gibt aber auch einige größere Anbieter, die sagt man auch bei den größeren Unternehmen eher dann zur An-

wendung kommen. Die haben meistens auch ein sag mal Standard, den sie mit ausliefern. Diese Software ist dann meistens auch sehr anpassbar, so dass man noch vieles für sich selbst zuschneiden kann wie man will. Aber dieses ich nehme dieses Modul und dieses Modul nehme ich nicht, kenne ich tatsächlich aus der Praxis selten und die Lösung sind meistens schon auch relativ gut zugeschnitten, dass die meisten Unternehmen, auch die meisten Teile davon brauchen. Da ist jetzt nicht viel dabei, was du nicht benötigen wirst. Da ist es eher andersrum, dass für spezielle Anwendungen, die sogar noch Zusatzmodule hinzunehmen musst. Wenn ich in Richtung Funktionstrennungskonflikte denke, die meisten IAM Lösungen können im Standard dies nicht wirklich tief für spezielle Software wie zum Beispiel SAP und da braucht man einfach Unterstützungslösungen. Also in der Praxis gibt alles. Ich bin aber der Überzeugung, dass man ja eigentlich immer Richtung Standardisierung der Prozesse gehen sollte und damit auch Standards ausrollen sollte. Das heißt, wenn ich für mich als Unternehmen, ich biete ja den im Service nicht an, weil ich das machen will, sondern es gibt ja gewisse Vorgaben und Standards im Unternehmen, die das Unternehmen auch einhalten will und wenn ich schon ein zentraler Service also einen IAM Service aufbaue, dann ist die Idee dahinter, auch die Standardvorgaben entsprechend komplett anzuwenden. Das heißt im Normalfall, um die eigenen oder gesetzliche Vorgaben als Applikation zu erfüllen, müsste ich theoretisch auch den Service im vollen Umfang auch entsprechend nutzen. Aber in Wirklichkeit ist es in der Tat so, dass man im Zweifel nicht alles nutzen kann. Es kann dafür unterschiedliche Gründe geben. Angefangen von Schnittstellen, die es vielleicht so einfach nicht gibt und die Umsätze der Schnittstelle zu teuer wäre, bis hin, dass das technisch im Zweifel nicht möglich ist, dass ich automatisiert die Accounts aus dem IAM Tool heraus anlegen muss oder darf, dann muss man so eine Lösung gehen. Aber wie gesagt, eigentlich bin ich eher davon überzeugt, dass man es vermeiden sollte.

I: Können Sie ein Beispiel dafür geben, wie Modularität in IAM-Services die Dienstleistung für interne und externe Kunden beeinflusst?

A: Zum Teil, habe ich ja die Frage schon beantwortet. Also ich bin eigentlich kein Freund davon nicht den vollen Scope auszurollen, denn man hat ja nicht umsonst diese Prozesse so definiert, weil die wahrscheinlich dann auch durch Regulierer wie die Bafin und Co. ja erst mal auf das Unternehmen auferlegt sind und vom Unternehmen einzuhalten sind. Aber ansonsten ist es wie gesagt auch aus besagten Gründen, da wo es nicht geht, muss man ja trotzdem irgendwie versuchen, die in die Vorgaben einzuhalten und da wäre es an sich schlecht sich nur Teile des Services für die Applikation nutzbar zu machen. Das ist aber vor allem, wenn ich an große Anbieter denke, ist nicht einfach. Vor allem in der Praxis, dann ein nur Teile davon verfügbar zu machen. Vor allem kann ich mir in der Tat nur schwer vorstellen, welchen Teil des klassischen IAM Services man dann abschneiden würde. Wenn man ein bisschen tiefer Richtung PAM vielleicht schaut, dann kann man dies innerhalb des IAM-Tools trennen, das meistens dann auch anderes Stück Software. Sobald du eigentlich an die Lösung angebunden bist, dann wüsste ich könnte ich mir schwer vorstellen, warum du eine der Kernfunktionalitäten oder Kernservices einer IAM-Lösung nicht nutzen solltest.

I: Inwieweit erfordern IAM-Services eine höhere Integrationsebene mit anderen Unternehmenssystemen?

A: Das ist super wichtig. Wir wissen alle, wie divers die Technologiewelt ist, aus Integrationsperspektive zumindest und das ist natürlich für die IAM Lösungen als zentrales Tool an dem im Best Case alle Applikationen anbindbar sein sollen, einfach kaum managebar in der Praxis ist es so, dass die großen Anbieter oder die bekanntesten, die haben ich sag mal klassischerweise drei, vier oder fünf Konnektoren oder Anwendungsmöglichkeiten im Standard schon implementiert. Natürlich klassische Sachen Richtung SAP sind meistens schon vorhanden, weil zumindest jetzt im deutschen Raum, gibt es wenig große Unternehmen, die kein SAP im Einsatz haben. Bzgl. Personaldate aber auch als ERP Lösungen. Was

auch klassisch immer oder meistens vorhanden ist, ist die Möglichkeit über Active Directory eine Connection aufzubauen. Dadurch dass wir uns immer stärker im Web bewegen, bitten die meisten dann auch die ein oder andere Schnittstelle für potenzielle Webapplikationen. Das heißt aber, dass die dann auch ein Standardkonnektor als Protokoll anbieten und die Software muss dann dafür sorgen, also sprich die Anwendung, die sich kann, anbinden lassen will, muss dafür sorgen, dass die damit entweder umgehen kann.

I: Wie priorisieren Sie Interoperabilität und standardisierte Protokolle im Kontext von IAM-Services?

A: Also ich bin Freund von Standard. Und zwar aus zwei Perspektiven die erste, sag mal die pragmatische servicegetriebene Perspektive ist, es machte es natürlich für Servicebetreiber einfacher einen Prozess zu haben, einen Standard zu haben, den man auf alle anwenden kann. Das ist von der Handhabung her natürlich deutlich einfacher. Wir haben auch einige Kunden von uns, die den IAM Service an ein IT-Tochter oder IT-Teams auslagern und die bieten es tatsächlich auch als Service an und durch den hohen Grad der Standardisierung gewisser Services oder Anbindungsmöglichkeiten sind die Aufwände tatsächlich sehr gering. Es macht es deutlich pragmatischer und auf der anderen Seite finde ich Standards auch deswegen wichtig, weil diese Prozesse, die wir mit IAM Einführen die sind meistens nur durch die Software nicht getan. Es gibt ja trotzdem noch im Hintergrund irgendeine interne Revision oder ein Information Security Management Team, die sich zusätzlich Kontrollaktivitäten auferlegt haben, um die Qualitäten auch sicherzustellen und gegenüber einem Dritten auch Aussagefähig zu sein und bei jeder Abweichung vom Standard müssen die Kollegen was zusätzlich machen. Die müssen für sich neue Kontrollen überlegen, die müssen schauen, wie die trotzdem einen gewissen Standard erreichen oder sich überlegen, wie sie Vorgaben erfüllen können. Das macht es für die zusätzlich noch schwieriger. Das heißt, wir haben eigentlich den die Betreiber des Services, der davon profitiert, nach Standards zu arbeiten, aber auch die die dann am Ende als 3rd Line of Defence die Kontrollen nochmal validieren, haben entsprechend auch ein einfacheres Leben. Nichtsdestotrotz, wie gesagt, lässt es sich leider nicht immer umsetzen.

I: Gibt es von Ihrer Seite aus Punkte, die noch nicht angesprochen wurden, die Sie aber hinzufügen möchten?

A: Insgesamt muss man sagen und es gibt tatsächlich Ansätze beispielsweise Service-Now auch als IAM-Tool zu nutzen. Die Herausforderungen ist es zu schauen welche Möglichkeiten diese Software mit sich bring. Einiges müsste man in einem klassischen ITSM-Tool vorerst nachbauen. Ich bin aber sehr gespannt auf deine Ergebnisse

I: Ich danke Ihnen aufrichtig für Ihre Bereitschaft und die Zeit, die Sie sich genommen haben, um ein Interview mit mir zu führen. Ich werde meine Ergebnisse voraussichtlich im September präsentieren.

Appendix 4: Interview Transcript II

General Data:

Interview-Type	**MS-Teams**
Interview-Number	**2**
Interview Date	**26.07.2024**
Interview-Duration (in Minutes)	**40min**

Demographic Data:

Industrial Sector	**Consulting**
Role	**Director**
Experience in IAM / ITSM (in Years)	**12 Jahre**

I: Vielen Dank, dass Sie sich heute die Zeit nehmen, ein Interview mit mir als Experten zu führen. Bevor wir mit dem Interview beginnen, möchte ich mich kurz vorstellen und Ihnen einige Informationen über mich geben. Mein Name ist Manuel Yambao und ich befinde mich in der Endphase meines Bachelorstudiums der Wirtschaftsinformatik an der Hochschule Ulm und der Hochschule Neu-Ulm. Im Rahmen des Interviews möchte ich Ihnen einige Fragen zu ITSM- und IAM-Diensten stellen. Wenn Sie damit einverstanden sind, bestätigen Sie bitte kurz. Wenn Sie keine Fragen haben, würde ich jetzt gerne mit dem Interview beginnen. Andernfalls können wir vorher etwaige offene Fragen klären.

I: Erzählen Sie mir bitte zu Beginn des Interviews von den allgemeinen Aufgaben, die Sie in Ihrem Unternehmen ausführen.

A: Ich bin seit insgesamt 3 Jahren Im Bereich Identity and Access Management für den DACH-Bereich primär und jetzt seit dem 1.7.2023 der leitende Director für das Thema Identity and Access Management, Assurance and Advisory. Soll heißen: Das ist die Kompetenz oder besser gesagt die Solution bei EY in der Serviceline Assurance und in der Sub Service Line Technology Risk, die sich mit dem Thema Identity and Access Management befasst, mit dem Fokus auf Governance Assurance. Hierbei werden unsere Kunden unterschiedlichster Sektoren beraten, gerade mit Blick auf Compliance, Risiko und Kontrollthemen im Bereich Identity und Access Management sowie artverwandten Disziplinen. Mit dem Blick auf Compliance, Risikoorientierung und Prüfungssicherheit nachhaltig in den Organisationen zu etablieren. Kundengrößen erstrecken sich von KMU-Bereich bis hin zu, und das ist unser Fokus, DAX 40 Mandate.

I: Welche Merkmale hat ein IAM-Service, der ihn von anderen IT-Services unterscheidet?

A: Ja, insbesondere hier nimmt man sich immer grundsätzlich als Enabler wahr und gerade mit dem Fokus auf Automatisierung, mit dem Fokus auf Effizienzsteigerung und mit dem Fokus auf wirkliche tatsächliche Unterstützung der primär wertschöpfenden Prozesse. IAM auf der anderen Seite tut dies auch, wenn es gut etabliert ist. Das bedeutet, durch eine höhere Automatisierung schnellere Prozessdurchlaufzeiten zu erwirken, Mitarbeiter schnell arbeitsfähig zu bekommen und Mitarbeiter auch tatsächlich zielgerichtet auf die Systeme entsprechend zuzulassen. Der Fokus von IAM ist primär allerdings der auf der Risikomitigierungen Seite. Das bedeutet, wir konzentrieren uns und IAM konzentriert sich insbesondere auf die Vermeidung von potenziellen Risiken im Kontext des Zugriffs auf Daten und Informationen einer Organisation. Soll heißen, der Fokus von IAM liegt dahin zu kontrollieren und zu regeln, dass im Umgang mit Informationen und Daten eine Kontrolleffektivität gewährleistet wird und eine saubere Governance eingehalten wird. Diese trägt dazu bei, dass Informationssicherheit gewährleistet werden kann und stellt somit einen wesentlichen Bestandteil bzw. eine wesentliche Säule der Informationssicherheit dar. Neben den performancesteigernden Aspekten, wobei primär das Thema der Risikomitigation im Vordergrund steht, gibt es unterschiedliche Arten von Risiken, also von den finanziellen Risiken bis hin zur Ausfallrisiken, bis hin zu Reputationsrisiken, die alle ein Stück weit durch ein effektives Identity and Access Management bedient werden. Soll heißen, wenn ich ein hohes Compliance Niveau habe, habe ich im Kontext ein geringeres Risiko von Compliance-Risiken. Wenn ich die Informationen sauber im Griff habe und auch nur den Mitarbeitenden oder auch technischen Identitäten der Zugriff auf Informationen gewähre, die sie haben sollen, ist das Risiko von einem missbräuchlichen

Umgang mit diesen Informationen, auch im Kontext einer eines Reputationsrisikos geringer. Und am Ende ist sowieso alles eine Art finanzielles Risiko, weil auch Risiken, wie die, die mir bewusst sind und die ich auch entsprechend berichte, gebundenes Kapital sind. Somit habe ich bei einem Missbrauch von Systemzugriffen durchaus auch das Risiko von Kapitalabfluss. Somit sehe ich folgenden Unterschied: Zu einem signifikanten Teil ist es ein performancesteigerndes und prozessunterstützendes Medium, was wir mit IAM bedienen. Der Hauptunterschied ist glaube ich, dass der Fokus auf der Risikomitigation und auf der Vereinheitlichung von Kontrollprozessen liegt.

I: Können Sie Beispiele dafür geben, wie IAM-Services auf häufige Applikations On- und -Offboardingprozesse reagieren?

A: Die grundsätzliche Maßgabe im Sinne eines sogenannten Einheitlichkeitsprinzips, was auch tatsächlich durch viele regulatorische Vorgaben, aber auch durch Risikomanagement und interne Governance Anforderungen passiert, ist grundsätzlich, dass man überhaupt auf einen zentralen IAM-Service wechselt. Hierzu gehört auch die Erreichung eines möglichst hohen Abdeckungsgrad von IT-Assets und dazu gehören zum einen Business Applikationen wie auch IT-Komponenten und Infrastruktur-Komponenten und zum anderen auch die klassischen Microservices und Webservices. Soll heißen, je mehr Services an diesem zentralen IAM-Prozess angebunden sind, desto effektiver und desto abdeckungsreicher ist das IAM. Somit kann ich die Effektivität von Identity und Access Management zu einem signifikanten Teil durch die Abdeckung der IT-Asset-Landschaft einer Organisation messen. Diese Messung kann dann durch den Abdeckungsgrad in der Breite und durch die Kontroll-Effektivität innerhalb der Prozesse erfolgen. Das Wesentliche ist, dass gerade durch Onboardings die Effektivität eines IAM-Services signifikant jedes Mal verbessert wird, weil der Abdeckungsgrad größer ist.

I: Wie unterscheidet sich die Verwaltung von Usern in IAM-Services von der in anderen IT-Services?

A: Es gibt Unterschiede, weil wir, insbesondere mit dem Abbild von Personen und digitalen, sowie technischen Identitäten, uns in einem anderen Lifecycle bewegen. Gerade wir im Identity Management, konzentrieren uns nicht unbedingt auf den Lifecycle von betrieblichen Anwendungen, Systemen, Services, Infrastruktur-Komponenten, sondern im Umgang mit sogenannten digitalen Identitäten. Wir fokussieren uns auf das digitale Abbild von Personen oder technischen Usern entlang ihres eigenen Lebenszyklus, das ist der sogenannte Joiner-Mover-Leaver Prozess. Der Joiner Prozess beschreibt den Eintritt einer Person in die Organisation oder die initiale Anlage einer technischen Identität, eines technischen Users dazu können zum Beispiel auch Robotik User zählen, um das Ganze vielleicht noch mal zu konkretisieren. Der Mover-Prozess beschreibt die Pflege von Identitäten, beispielsweise bei einem Abbild von natürlichen Identitäten wäre das eine Struktureinheit oder ein Abteilungswechsel innerhalb der Organisation bis hin zum Leaver-Prozess, welcher den Eintritt beispielsweise in die Rente oder das Verlassen einer Firma im Rahmen einer Kündigung oder den Eintritt in eine Altersteilzeit oder in eine temporäre Abwesenheit im Rahmen von Sabbaticals oder einer Elternzeit beschreibt. Also der Fokus ist im Identity Management im Gegensatz zu anderen IT-Services nicht auf den Asset selbst, sondern eher auf den Nutzen, den Identitäten, die diese IT-Services selbst nutzen.

I: Welche Strategien würden Sie einsetzen, um die Skalierbarkeit von IAM-Diensten zu gewährleisten?

A: Die grundsätzliche Strategie, die ich einsetzen würde, wäre der Fokus auf Themen, die sowieso gerade in aller Munde sind, wie zum Beispiel Themen wie Machine Learning und Artificial Intelligence. Weil viele Themen, die wir momentan als kontrolleffektive Basis ansehen, und zwar das Wissen von Mitarbeiter Kompetenzen innerhalb einer Organisation, erfolgt nach wie vor immer noch rein manuell und manchmal sogar auf Basis von Experten. Das bedeutet nicht, dass die Kontrolleffektivität darunter unbedingt leiden muss, aber es muss sich auf die Verantwortlichkeit von Personen im Unternehmen verlassen werden, was korrekt und richtig ist, aber es hat damit immer noch einen erhöhten Bedarf an

manuellen Eingriffen, somit auch ein Verlassen auf Wissen und Kompetenzen von Personen innerhalb der Organisation. Wenn wir das ganze Thema uns strategisch anschauen, sage ich oft, dass Identity and Access Management dann am besten ist, wenn man es nicht merkt. Ein höheres Automatisierungspotential und eine höhere Effektivität und Effizienz in den Prozessdurchlaufzeiten durch einen Abgleich von Informationen und dementsprechend auch einer Kontrollentscheidung, beispielsweise in der Vergabe von Zugriffen von Mitarbeitern aus Systemen, durchaus auch durch Attribute und dementsprechend auch über Machine Learning künftig abbilden. Das hat meines Erachtens 2 Effekte: Es hat den positiven Effekt des schnelleren Herstellens der Arbeitsfähigkeit der Mitarbeitenden oder grundsätzlich der Identitäten. Das hat aber auch den Effekt, dass anhand von klaren Interpretationen von Attributen und Daten der Zugriff anhand von Regeln immer einheitlich getroffen werden kann. Die Einheitlichkeit und Standardisierung anhand von Regeln im Identity and Access Management stützt die Effektivität und die Kontrolleffektivität des Identity und Access Management erheblich. Es gibt auch Einschränkungen, so kann ich zum Beispiel nicht ein Identity and Access Management auf einer grünen Wiese aufbauen, indem ich nur rein attributbasiert den Zugriff auf Systeme ermögliche. Das hat man mal probiert, im Rahmen des sogenannten Attribute Based Exit Control oder Policy based access controls. Das funktioniert meines Erachtens nur ab einem gewissen Reifegrad eines Identity and Access Management, wie wir es den traditionellen kennen. Soll heißen, die Strategie ist nicht eine initiale Neuausrichtung auf Artificial Intelligence Policies oder Attribut basierten Zugriffen, sondern ist meines Erachtens eine Weiterentwicklung eines Identity and Access Managements im traditionellen Sinne auf Basis beispielsweise von einem Role Based Access Control gerade in der Richtung, die uns beispielsweise durch AI geboten wird.

I: Wie gehen Sie mit variablen Userlasten um und welche Rolle spielt die flexible Ressourcenzuweisung in diesem Zusammenhang?

A: Meines Erachtens gehen die unterschiedlichen Lösungen auseinander und es verbietet mir leider aus Independence Gründen zu sagen, welche Lösung das besser und welche das schlechter kann. Aber es gibt durchaus Unterschiede von proprietären Lösungen am Markt, die dann mit unterschiedlichen Datenstrukturen und mit unterschiedlichem Load balancing, anders mit Dingen umgehen. Aber grundsätzlich ist immer das Thema, je komplexer ein Kontrollset innerhalb einer IAM Lösung aufgesetzt ist, desto Signifikanter sind die Einflüsse auf die Tool Performance, plus die klare Maßgabe für eine Lösung sollte sein, gerade mit solchen Peaks balancieren sauber umzugehen, weil der Zugriff und vor allen Dingen auch die Anzahl von Prozessen, die über eine IAM Lösung läuft, nicht stetig ist, sondern insbesondere gerade, liegt in der Natur der Sache, bei Jahreswechseln, Monatswechseln, tendenziell auch an den Wochentagen, meistens entweder Anfang der Woche oder Ende der Woche, meistens dort Peaks entstehen und mit diesen Peaks muss durch ein sauberes Balancing und auch durch eine entsprechende variable Zuordnung von Systemressourcen müssen diese Peak sauber abgefangen werden, insbesondere auch um die Usability für die Endanwender sicherzustellen.

I: Wie definieren Sie 'hohe Effektivität im Kontext des Availabilitymanagement für IAM-Services?

A: Eine Effektivität im Sinne der Availability würde ich klassisch auch auf Basis der Availability, nämlich auf der Hochverfügbarkeit eines IAM Systems sehen, und zwar du hattest vorhin das Thema mit Flexibilität angesprochen und ein IAM Service muss auch auf Ad hoc Anfragen reagieren können, soll heißen, ich brauche zum Beispiel auch mal am Wochenende einen ad hoc Zugriff auf eine Systemressource, das ist meines Erachtens dann nur Bewerkstelligbar, wenn ich eine Hochverfügbarkeit im Sinne von einer 99% Availability habe. Im Bezug auf die Effektivität: Wenn der IAM Service über die Standardkontroll-Prozesse nicht verfügbar ist, sucht sich derjenige, der auf diese Systemressource Zugriff haben muss, Analog vom Wasser immer den geringsten Widerstand und den einfachsten Weg, und das bedeutet verlassen von standardisierten Kontrollprozessen, was wiederum zu Lasten der Effektivität eines

Identity und Access Managements geht, weil eine Effektivität von Identity und Access Mensch lebt davon, dass im Idealfall jeglicher Zugriff über die Standardkontrollprozesse erfolgt.

I: Welche spezifischen Mechanismen würden Sie einsetzen, um die Kontinuität für IAM-Services zu gewährleisten?

A: Es gibt Mechanismen im Sinne dessen, dass wir grundsätzlich ja für alle Systeme und wir haben hier ein System, was durchaus auch eine kritische Säule auf der gesamten IT-Infrastruktur darstellt. Somit gibt es klassische Backup und Recovery Mechanismen analog anderer sensibler und signifikant und kritischer IT-Systeme, natürlich auch für das IAM-System. Folglich sind viele neue und jetzt gerade auch proprietäre Lösung am Markt, die als Webservice angeboten werden, die mit virtuellen Backup und Recovery Mechanismen arbeiten, die nahezu hundertprozentige Verfügbarkeit eines IAM-Services nachhaltig sicherstellen sollen.

I: Wie wird Modularität im Servicedesign von IAM-Diensten implementiert, um den vielfältigen Bedürfnissen der Kunden gerecht zu werden?

A: Ich nehme die Perspektive eines IAM Services ein und ich mach ein narrow-down wirklich auf das Thema des Onboardings. Und ich nehme die Perspektive jetzt mal der Kundenseite, also der Applikationsseite an. Ich hatte vorhin schon von den unterschiedlichen Anbindungsvarianten oder Onboarding Varianten von Applikationen und Services gesprochen. Das Ziel ist und sollte sein, möglichst über standardisierte Konnektoren die Anbindung und auch Abbildung von Services und Anwendungen auf der IAM-Lösung sicherzustellen. Ich denke das bekannteste Thema ist glaube ich das AD first, das auch meistens in vielen IT-Organisationen oder in vielen IT-Bereichen der Organisation, eine klare strategische Maßgabe ist, nämlich die Anbindung von Business Applikationen und Services über ein Verzeichnis Dienst Active Directory oder Azure AD etc. zu gewährleisten. Das bedeutet, das ist das, was die Anwendung von ihrer Perspektive tun und dementsprechend muss IAM auch darauf reagieren und diese Konnektoren auf der IAM Seite selbst analog ebenso zur Verfügung stellen. Also je größer und heterogener die Systemlandschaft ist, desto wichtiger ist es, dass sich IAM auf der Art und Weise auf dieser Heterogenität der Systemlandschaft auch aufstellt und das entsprechend zu bedienen. Habe ich ein SAP-System, brauche ich ein SAP Standard Connector, habe ich ein Oracle System, brauche ich einen Oracle Standard Connector, habe ich eine Postgresdatenbank, brauche ich einen Postgres Standard Connector, um einfach die Hürde des Onboardings möglichst niedrig zu halten und darum wieder eine möglichst hohe Abdeckung von IAM über die Systemlandschaft der Organisation sicherzustellen.

I: Können Sie ein Beispiel dafür geben, wie Modularität in IAM-Services die Dienstleistung für interne und externe Kunden beeinflusst?

A: Insbesondere mit dem Fokus auf Customer Identity und Access Management hat es meines Erachtens die Nutzung von der Kundenseite für organisationsspezifische Services grundsätzlich verändert, weil es hat die Rolle des Kunden in der Nutzung der Services, die eine Organisation im B2C Bereich den Kunden anbietet in einer grundsätzlichen Art und Weise völlig verändert, weil er ist jetzt nicht mehr der reine Konsument eines Services im Sinne von er liest, er nutzt Informationen, die in die Organisation im B 2 C Umfeld bereitstellt, sondern er ist im Endeffekt wie damals der klassische interne Enterprise User auch eine Identitätsklasse, die tatsächlich auch Änderungen in den Informationen in Stammdaten und Kundenstammdaten selber vornehmen kann. Das hat 2 Effekte, das hat einmal den Effekt, dass mitunter eine größere Aktualität der jeweiligen Daten gewährleistet werden kann. Auf der anderen Seite natürlich aber auch das Risiko des Missbrauchs und gegebenenfalls auch das Risiko im Sinne der schwindenden Daten und Informationsintegrität, die natürlich halt auch größer ist. Soll heißen Vorteile durch CIAM andere, beziehungsweise aktivere Rolle der Kunden auf den Systemen der Organisation und damit verbunden aber auch eine höhere Kontrollanforderung, um eine Datenintegrität und auch

Vertraulichkeit im Sinne der klassischen Schutzziele entsprechend auch sicherzustellen, weil es sind eben gerade nicht nur die Personenkreise der internen Mitarbeiter, der externen Dienstleister, der Partner, sondern es kommt noch eine weitere, und zwar eine signifikant größere Gruppe dazu, nämlich die der Kunden an sich.

Das Thema mit der Modularität in dem Moment zielt natürlich ab auf entweder ein zentrales, individuelles Identity und Access Management, was organisatorisch spezifisch ist. Aber, und da gab es auch in der Vergangenheit mehrere Ansätze, das nannte sich dann Unified ID und die Möglichkeit, über eine zentrale Identitätenplattform eigentlich das für Personen außerhalb einer Organisation sicherzustellen, was man schon für interne Mitarbeiter hat. Eine Identität ist ja nichts anderes als die Sammlung von Attributen, die eine Person, wie es schon sagt, identifiziert das meistens für interne Mitarbeiter ist das das HR-System, für externe Mitarbeiter ist es ein Identity Hub, beispielsweise im Sinne eines SAP Field Class, beispielsweise für externe Kunden gab es das bislang in der Art und Weise noch nicht. Und diese Idee einer Unified ID ist im Grunde genommen genau das, eine Plattform sicherzustellen, um beispielsweise über eine dedizierte Plattform oder beispielsweise Themen wie Google wie Facebook, Apple, etc. wo diese Informationen bereits ja schon gesammelt sind und verschlüsselt halt für Authentisierungsmechanismen dem jeweiligen Service zur Verfügung gestellt werden, um dem User es möglichst einfach zu machen mit seinen Identitätsattributen den jeweiligen Service zu können.

I: Inwieweit erfordern IAM-Services eine höhere Integrationsebene mit anderen Unternehmenssystemen?

A: Je höher die Integration, desto effektiver ist das System. Ich gebe Beispiele: Wenn Ich eine Provisionierung, also die Umsetzung von Systemzugriffen auf eine Anwendung rein manuell habe. Beispielsweise es werden sogenannte Provisionierung oder Deprovisionierungsaufträge an ein manuelles User Management übermittelt, beispielsweise im Sinne von Tickets Service-Now Und ein Mitarbeiter, ein User Manager oder ein Benutzeradministrator setzt dies manuell um, sowohl in Züge als auch vergaben, sowohl Sperrungen als auch Accountanlagen. ist das natürlich mit jedem Handgriff, der manuell erfolgt, fehleranfälliger. Nächste Integrationsstufe wäre beispielsweise ein lesender Konnektor, soll heißen ich lese die Zugriffe aus einem System aus und habe darüber einen Soll-Ist-Abgleich, eine Reconciliation Funktion bis zum gewissen Grad schon mal sichergestellt. Eine Vollintegration ist zum Beispiel eine synchrone Anwendung, wo es heißt sowohl der IAM Service schreibt aktiv Provisionierung rein und liest sie gleichzeitig aus und balanciert sie zwischen SOLL und IST mit einem führenden IAM Service als SOLL so aus, dass das, was im Zielsystem in der Ziel Anwendung drin ist, denen genehmigten SOLL, gemäß des IAM Services entspricht, soll heißen, je höher die Integration, desto höher die Möglichkeit der Prozesseffizienz und desto höher die Möglichkeit auch der Kontrolleffektivität.

I: Wie priorisieren Sie Interoperabilität und standardisierte Protokolle im Kontext von IAM-Services?

A: Einheitlichkeit, Standardisierung sind dadurch gekennzeichnet, dass es verprobte technische Mechanismen sind, die, wenn sie standardisiert und fokussiert sind, soll heißen, je weniger Wege ich habe, wie Informationen von Zielsystemen in den IAM Service reinkommen beziehungsweise aus dem IAM Service in die jeweiligen Um-Systeme kommen. Je standardisierter und vor allen Dingen weniger diese Themen sind, desto einfacher ist es zu kontrollieren, desto geringer ist die Fehleranfälligkeit und desto geringer ist das Risiko von Verlusten im Sinne der Datenintegrität. Und dementsprechend halt auch die Effektivität des IAM-System als Ganzes. Somit wäre die Priorisierung Standardisiert vor Individuell vor Manuell. Also standardisiert vor individuell und das vor manuell.

I: Interviewabschluss: Gibt es von Ihrer Seite aus Punkte, die noch nicht angesprochen wurden, die Sie aber hinzufügen möchten?

A: Ich würde gerne noch erwähnen, da ich das Thema zum Backup und Recovery interessant fande, dass viele Großorganisationen, gerade aus Performance Gründen, noch on Prem Lösungen nutzen, da diese davon überzeugt sind, dass die Performance höher sein soll. Dies liegt daran da eine größeren Anpassungspotenzial vorhanden ist. Die On-Prem Lösungen waren in der Vergangenheit dadurch gekennzeichnet, dass „IT Follows Business“ als Maßgabe vorhanden war, das bedeutet man hat die Prozesse der Organisation bzw. den IAM Service den Prozessen der Organisation angepasst. Das was wir gerade angeführt haben bzgl. Availability und Loadbalancing etc. und alles was als Cloud Service gerade neu in den Markt strömt, bringt dies alles mit, gerade weil Cloud individuell und je nach Bedarf Ressourcen zur Verfügung stellt und durch ein Loadbalancing, Backup und Recovery viele der Themen abdeckt. Ein signifikanter Nachteil, Stand heute, ist dass es in der Regel eine sehr standardisierte Lösung ist, wo nun die Maßgabe ist „Business follows IT“. Das Business muss sich quasi nun an das IAM angleichen. Das zu balancieren wird glaube ich sehr spannend in der Zukunft, weil viele Organisationen dies nicht „gewöhnt“ sind. Aber um Usability zu haben muss es irgendwo zum Konsens laufenm dass Organisationen die gesamten Vorteile von IAM Cloud Services nutzen können.

I: Ich danke Ihnen aufrichtig für Ihre Bereitschaft und die Zeit, die Sie sich genommen haben, um ein Interview mit mir zu führen. Sollten Sie an den Ergebnissen meiner Bachelorarbeit interessiert sein, werde ich Sie im September darauf ansprechen und sie Ihnen präsentieren.

Appendix 5: Interview Transcript III

General Data:

Interview-Type	**MS-Teams**
Interview-Number	**3**
Interview Date	**29.07.2024**
Interview-Duration (in Minutes)	**20min**

Demographic Data:

Industrial Sector	**Consulting**
Role	**Consultant / Auditor**
Experience in IAM / ITSM (in Years)	**3 Jahre**

I: Vielen Dank, dass Sie sich heute die Zeit nehmen, ein Interview mit mir als Experten zu führen. Bevor wir mit dem Interview beginnen, möchte ich mich kurz vorstellen und Ihnen einige Informationen über mich geben. Mein Name ist Manuel Yambao und ich befinde mich in der Endphase meines Bachelorstudiums der Wirtschaftsinformatik an der Hochschule Ulm und der Hochschule Neu-Ulm. Im Rahmen des Interviews möchte ich Ihnen einige Fragen zu ITSM- und IAM-Diensten stellen. Wenn Sie damit einverstanden sind, bestätigen Sie bitte kurz. Wenn Sie keine Fragen haben, würde ich jetzt gerne mit dem Interview beginnen. Andernfalls können wir vorher etwaige offene Fragen klären.

Erzählen Sie mir bitte zu Beginn des Interviews von den allgemeinen Aufgaben, die Sie in Ihrem Unternehmen ausführen.

A: Genau, ich bin Berater bei im Bereich Technology, Risk und bin da sowohl in der Prüfung als auch in der Beratung von Informationssicherheitsprüfung und anderen Beratungsprojekten tätig, vor allem mit regulatorischem Hintergrund. Das heißt, primär konzentriere ich mich darauf, dass wir in Deutschland und der EU betroffene Unternehmen durch Regularien dabei unterstützen, eben compliant zu werden, das heißt im weitesten Sinne sind wir dabei beschäftigt, ein ISMS mit aufzubauen, ein ISMS zu verbessern, ISMS zu prüfen, um eben festzustellen, wo sich gegebenenfalls strukturell etwas ändern oder verbessern lässt. Allgemein weniger auf der technischen Ebene und primär auf Governance Ebene.

I: Welche Merkmale hat ein IAM-Service, der ihn von anderen IT-Services unterscheidet?

A: Also ich glaube, dass dem I am im weitesten Sinne dann doch besondere Aufgaben zukommen und ein spezieller Need das sich eine Organisation an sich selbst. Das heißt, IAM adressiert ganz spezifische Risiken für sich selbst das genau nur den Abschnitt bearbeitet, dass sich um die Berechtigungsvergabe und Identitäts- und Berechtigungsverwaltung kümmert. Andere IT-Services können natürlich viel umfangreicher oder auch teilweise genauso „nischig“ sein. Ich würde sagen es ist ein sehr zentraler und sehr wichtiger Service innerhalb eines Unternehmens, da es Ebene sehr wichtige ist oder zentrale Aufgabe übernommen werden, um überhaupt andere Services auch zu ermöglichen.

I: Können Sie Beispiele dafür geben, wie IAM-Services auf häufige Applikations On- und -Offboardingprozesse reagieren?

A: Grundsätzlich könnte der IAM Service so gestaltet sein, dass er eben sehr universell ist und dann auch gut anwendbar ist. Das gleich im Umkehrschluss kann das auch auf die Anwendung zutreffen, die angebunden werden soll. Das heißt, wir müssen prüfen, inwiefern bestimmte Schnittstellen und die Kompatibilität eben möglich ist zwischen. Man muss sich im Klaren sein, was migriert werden muss oder was nicht migriert werden muss. Wenn es jetzt aber generell ums Onboarding oder Anknüpfung an IAM geht, ist die Frage, inwiefern können bestimmte Vorgaben, die sich ein Unternehmen an Anwendungen stellt, tatsächlich umgesetzt werden und inwiefern kann der IAM Service tatsächlich mit der Anwendung zusammen arbeiten? Also wie sieht es aus mit dem Incident Management Prozess oder Emergency User aus? Wie sieht es aus bei den Zugriffen? Wie wird die Authentifizierung gestaltet, vielleicht auch mit Protokollierung etc. und das muss dann entsprechend für jede Anwendung neu evaluiert werden.

I: Wie unterscheidet sich die Verwaltung von Usern in IAM-Services von der in anderen IT-Services?

A: Grundsätzlich würde ich sagen, würde ich das immer von der Risiko- oder von der Kontrollperspektive betrachten. Dementsprechend entstehen eigene Anforderungen, welche Zielsetzungen erfüllt werden sollen. Danach richten sich dann eben Prozesse wie z.B. Verwaltung von Usern, nachdem sich am Ende auch angebundene Applikationen halten müssen. Wenn man jetzt zum Beispiel irgendwelche konkreten gesetzlichen Anforderungen oder Sicherheitsanforderungen erfüllen möchte, kann dies der Zielsteuerung helfen, was der IAM Service am Ende leisten muss und das unterscheidet sich natürlich auch von anderen IT Services, die dann vielleicht auch wieder andere Anforderungen und andere Treiber haben, warum es diese gibt oder warum diese so oder so umgesetzt sein müssen.

I: Welche Strategien würden Sie einsetzen, um die Skalierbarkeit von IAM-Diensten zu gewährleisten?

A: Ich würde erstmal sagen, grundsätzlich ist es sinnvoll, einen zentralen Ansatz zu haben. Das heißt, dass man grundsätzlich versucht, ein zentrales Benutzermanagement aufzubauen und eine zentrale Benutzerverwaltung und dabei auch, vor allem dann von der Governance Perspektive einen guten zentralen Rahmen schafft, nachdem sich alles am Ende des Tages richten muss.

I: Wie gehen Sie mit variablen Userlasten um und welche Rolle spielt die flexible Ressourcenzuweisung in diesem Zusammenhang?

A: Da fehlt mir aus Governance Beratung und Audit Sicht leider das technische Wissen.

I: Wie definieren Sie 'hohe Effektivität im Kontext des Availabilitymanagement für IAM-Services?

A: Da denke ich, ist es wichtig, dass man sich einmal überlegt, was vielleicht eine Mindestbaseline ist, die getroffen werden muss. Das heißt, wir müssen einmal schauen, welcher die Demand denn eigentlich erfüllt sein muss und jetzt gerade aus Auditbrille ist eben der Teil abzudecken. Dass wir für uns identifizieren müssen, welche Risiken vorhanden sind und welche Risiken zutreffen könnten und anhand welchen Maßstabes bestimmte Dinge umgesetzt sein sollten oder müssten, um eben mindestens diese Risiken gewissermaßen zu mindern oder abzudecken. Das heiß die Effektivität oder auch die Wirksamkeit des IAM Services nicht quasi per se einfach festzulegen, sondern das immer entsprechend individuell und richtet sich nach der entsprechenden Nachfrage beziehungsweise den entsprechenden Risiken oder auch zum Beispiel bei der Verfügbarkeit eben nach dem, was tatsächlich eigentlich abgedeckt sein soll oder vorhanden sein soll. Entsprechend ist anhand dieser Nachfrage oder an diesen Anforderungen, dann eben auch zu definieren, was eben vorliegend sein muss, um eben eine gewisse Effektivität oder Wirksamkeit feststellen zu können.

I: Welche spezifischen Mechanismen würden Sie einsetzen, um die Kontinuität für IAM-Services zu gewährleisten?

A: Da ich viel mit Standards gearbeitet habe, ist denke ich ein wichtiger Punkt, dass eben ausreichend Ressourcen vorhanden sind. Das heißt, wir müssen zum einen Geld zur Verfügung haben, um eben etwas sicherzustellen und umzusetzen, aber auch Humanressourcen, das heißt, wir müssen genügend Mitarbeitende haben, die eben das Ganze am Ende mit umsetzen können und grundsätzlich auch noch andere organisatorische Ressourcen, ob es jetzt irgendwelche Rechenzentren, Verfügbarkeiten oder ähnliches sind. Je nachdem, was eben benötigt wird. Dann als nächsten Punkt bräuchten wir ausreichend Kompetenzen. Das heißt, wir müssen auch entsprechende Skillsets im Personal haben, um das Ganze umsetzen zu können. Es muss eine gewisse Kommunikationseben sichergestellt sein, um ein IAM Service am Ende zu erbringen und eben auch das Ganze aufrechtzuerhalten. Das Ganze muss ausreichend dokumentiert sein. Das heißt wir müssen entsprechende Vorgaben haben. Wir müssen entsprechende Prozesse auch dokumentieren, damit nicht jeder irgendwas macht, sondern das einheitlich gelebt werden kann und zum Schluss auch eine gewisse Awareness, dass für die gesamte Organisation diese Prozesse und Anforderungen auch kommuniziert werden können.

I: Wie wird Modularität im Servicedesign von IAM-Diensten implementiert, um den vielfältigen Bedürfnissen der Kunden gerecht zu werden?

A: Grundsätzlich ist für IAM mich ja nur in Anführungsstrichen eine Teildisziplin von ISMS, aber ich denke würde das Ganze anhand eines konkreten Prozesses beziehungsweise Lifecycles aufzeigen. Das heißt, ich würde es festmachen an beispielsweise einem Joiner Prozess, an einem Leaver Prozess oder einem Mover Prozess, an dem ich dann eben bestimmte Module aufbaue, dort würde ich es nicht nur nach IAM Disziplinen aufteilen, sondern vielmehr danach welche Use Cases sich in dem Unternehmen eben stellen oder in der Organisation, die eben nutzen von dem IAM Service hat.

I: Können Sie ein Beispiel dafür geben, wie Modularität in IAM-Services die Dienstleistung für interne und externe Kunden beeinflusst?

A: Erneut kann ich dazu leider keine konkrete Antwort geben.

I: Inwieweit erfordern IAM-Services eine höhere Integrationsebene mit anderen Unternehmenssystemen?

A: Deutlich hören, weil wir jetzt bei einem normalen System natürlich immer nur den Fall haben, dass es eben nur da ist, um seinen bestimmten Anwendungszweck zu erfüllen und auch zum Beispiel nur

einer bestimmten Business Unit vielleicht angewendet werden muss oder eben einem bestimmten Kreis und bei dem IAM Service ist natürlich deutlich allgemeiner, weil es ein zentraler oder ein Prozess für die gesamte Organisation in jeder Hinsicht sein muss und auch nicht anders eigentlich sein kann, weil die entsprechenden Risiken oder auch die Zielsetzung, die eben ein IAM Service für sich selbst hat nicht ein Teil einer Business Unit adressieren, sondern eigentlich die gesamte Organisation. Entsprechend sind die Anforderungen an die Integration viel höher, weil immer die Schnittstelle zu jeder anderen Anwendung mit betrachtet werden muss und eben aber auch immer die ganzen Anforderungen, die sich das IAM zum Beispiel durch eine Richtlinie oder durch einen bestimmten Standard etc. setzen sich das in jeder Hinsicht gefragt werden muss und dann gegebenenfalls, weil die Wahrscheinlichkeit, dass das bei bestimmten anderen Services nicht der Fall ist, dass diese Anforderungen erfüllt werden können, dass da eben nach einem Workaround gesucht werden muss und geprüft werden muss, wie bestimmte Sachen am Ende doch umgesetzt werden können und ich denke gerade diese Workarounds oder diese Sonderfälle, bei denen vielleicht ein Prozess oder die Umsetzung nicht nach Schema laufen kann, ist eben eine besondere Herausforderung dann auch bei der Integration. Aber grundsätzlich hat es natürlich einen sehr hohen Aufwand, weil eben die Integration überall in der gesamten Organisation erfolgen muss und falls das zu aufwändig ist, dann entsprechend halt risikobasiert, aber am Ende sollte Zielsetzung immer sein, den gesamten Roll out zu haben.

I: Wie priorisieren Sie Interoperabilität und standardisierte Protokolle im Kontext von IAM-Services?

A: Ja, also zum einen müssen die Anforderungen eben, wie ich vorhin meinte, genauso liegen, dass sie das Nötigste sicherstellen und gleichzeitig müssen sie aber auch so präzise sein, dass die Varianz der Sachen, die am Ende umgesetzt werden oder der Maßnahmen nicht hoch wird, sondern es muss eben eine Baseline umgesetzt sein, die auch einheitlich ist und dabei hilft dann zum Beispiel ja gerade so ein Governance Rahmen den man sich selber setzt, um den dann am Ende umzusetzen und die Priorisierung muss dann am Ende zwangsläufig irgendwie risikogesteuert sein.

I: Interviewabschluss: Gibt es von Ihrer Seite aus Punkte, die noch nicht angesprochen wurden, die Sie aber hinzufügen möchten?

A: Von meiner Seite aus wäre ich fertig.

I: Ich danke Ihnen aufrichtig für Ihre Bereitschaft und die Zeit, die Sie sich genommen haben, um ein Interview mit mir zu führen. Sollten Sie an den Ergebnissen meiner Bachelorarbeit interessiert sein, werde ich Sie im September darauf ansprechen und sie Ihnen präsentieren.

Appendix 6: Interview Transcript IV

General Data:

Interview-Type	**MS-Teams**
Interview-Number	**4**
Interview Date	**30.07.2024**
Interview-Duration (in Minutes)	**33min**

Demographic Data:

Industrial Sector	**Consulting**
Role	**Manager**
Experience in IAM / ITSM (in Years)	**7 Jahre**

I: Vielen Dank, dass Sie sich heute die Zeit nehmen, ein Interview mit mir als Experten zu führen. Bevor wir mit dem Interview beginnen, möchte ich mich kurz vorstellen und Ihnen einige Informationen über mich geben. Mein Name ist Manuel Yambao und ich befinde mich in der Endphase meines Bachelorstudiums der Wirtschaftsinformatik an der Hochschule Ulm und der Hochschule Neu-Ulm. Im Rahmen des Interviews möchte ich Ihnen einige Fragen zu ITSM- und IAM-Diensten stellen. Wenn Sie damit einverstanden sind, bestätigen Sie bitte kurz. Wenn Sie keine Fragen haben, würde ich jetzt gerne mit dem Interview beginnen. Andernfalls können wir vorher etwaige offene Fragen klären. Erzählen Sie mir bitte zu Beginn des Interviews von den allgemeinen Aufgaben, die Sie in Ihrem Unternehmen ausführen.

A: Mein Arbeitsalltag setzt sich aus meiner Sicht zusammen aus drei großen Säulen. Säule eins ist Project Delivery im Bereich IAM bei den Kunden. Säule zwei ist internes Engagement Management. Damit meine ich das Pflegen und Verwalten der Financials, also Rechnungsstellung, Weiterbeauftragung, Jobpflege, Planung, Ressourcenplanung auch und Säule drei ist Mitarbeiterentwicklung. Dann könnte man noch eine vierte Säule hinzunehmen, die hätte ich jetzt in der ersten integriert, da könnte man noch das Thema Accountentwicklung und Marktbearbeitung hinzufügen. Je nachdem, wo du das ein kategorisieren möchtest, sind das die großen vier Dinge, die wir, glaube ich, ab Manager fängt das an, haben.

I: Welche Merkmale hat ein IAM-Service, der ihn von anderen IT-Services unterscheidet?

A: Ich glaube, dass IAM einer der wenigen Services ist, wenn man den vergleicht gegenüber anderen Services nimmt, egal ob jetzt aus Dienstleister oder Mitarbeiter Sicht eines Unternehmens sieht in irgendeiner Art und Weise diesen Prozessen, die von einem IAM vorgegeben werden leben muss, weil jeder Mitarbeiter in jedem Unternehmen in der heutigen Zeit braucht IT-Unterstützung bzw. jedes Unternehmen braucht für das Managen der wertschöpfenden Prozesse IT-Unterstützung und dafür müssen Mitarbeiter mit Berechtigung versehen werden, auf welchem Weg auch immer. Das heißt, im Normalfall wird jeder Mitarbeiter involviert, im Optimalfall merkt er es nicht. Das ist auch die Downside an dem Thema. Ein optimales IAM verläuft lautlos und der Mitarbeiter, der nicht primär mit dem Thema IAM in Berührung kommt, merkt es erst, wenn etwas nicht funktioniert. Deswegen werden wir mit IAM nie einen richtigen Preis gewinnen. Ein zweiter Teil, der sich auf das Thema IAM anwenden lässt, das geht auch so ein bisschen in das Thema Risikomanagement, aber bei IAM ist der Mehrwert, den wir

dem Unternehmen gegenüber schaffen oder der Mehrwert, den die Leute innerhalb eines Unternehmens, die IAM betreiben, gegenüber ihrem eigenen Unternehmen schaffen, schwer messbar ist. Es ist sehr schwierig, einen monetären Nutzen an das Thema IAM zu hängen. Warum? Weil wenn dein IAM gut funktioniert, hat man eigentlich keine Incidents, es gibt wenig Missbrauch, es ist smooth, du hast einen effizienten Weg, aber es ist extrem schwierig, bis unmöglich das mit einem monetären Wert zu beziffern. Das heißt, die Belohnung ist eigentlich, dass du Incidents minimierst, die du gar nicht hast, und die Schäden, wenn du einen Incident hast, möglichst gering bleiben. Das heißt, auch da das Thema IAM wird genau dann so richtig heiß, wenn es mal schief gegangen ist und es vorher nicht in Place war. Das ist leider so ein bisschen die Öde, die wir alle, die im Bereich IAM arbeiten tragen und da muss man, einfach Awareness erzeugen, dass das Thema durchaus eine Berechtigung hat.

I: Können Sie Beispiele dafür geben, wie IAM-Services auf häufige Applikations On- und -Offboarding-prozesse reagieren?

A: Es sind drei Themen, die wir oder die auch ich bei den Kunden befürworte und versuche zu bewerben. Punkt eins ist, wir brauchen einen Standard-Prozess zum schnellen On-Boarding. Das haben viele Unternehmen schon nicht. Was meine ich damit? Eigentlich müsste man das Thema IAM-On-Boarding in den allgemeinen Application-Life-Cycle-Prozess der IT von Unternehmen integrieren. Heißt, wenn ein Unternehmen eine neue Software einführt, dann gibt es im Normalfall Prozesse, wo Konzepte abgelegt werden. Es werden vorher Analysen gefahren, gegebenenfalls gegen das Enterprise Architecture Management, wo man sich die Gesamt-IT-Landschaft anschaut. Es werden dort gewisse Dinge abgefragt vor Go-Live einer Anwendung oder eines Services. Eigentlich muss das Thema IAM dort schon mit eingeflochten werden. Beispiel, das Schönste, was ich bisher gesehen habe, ist dass ein Unternehmen, die hatten ein sogenanntes Change Advisory Board. Das heißt, wenn ich als Service oder Anwendungsverantwortlicher mit einem neuen Service live gehen möchte, dann muss ich mir einen Slot in diesem Boardtermin buchen welcher periodisch stattfindet. Dann habe ich ca. zehn Minuten Zeit zu erklären, warum ich live gehen möchte und was ich da tue. Dieses Change Advisory Board setzt sich zusammen aus Leuten, aus Enterprise Architecture, aus Risk Management, aus Governance, also einfach eine Auswahl an ausgewählten Leuten, die die IT-Infrastruktur des gesamten Unternehmens aus unterschiedlichem Blickwinkel betrachten. Das Unternehmen, das das gemacht hat, hatten eine Person aus dem IAM-Team mit dabei in diesem Change Advisory Board. Das heißt, das IAM-Team hat zu jeder Zeit mitbekommen, wenn es neue Services oder neue Anwendungen gab. Diese Person hat sich dann Anwendungsverantwortlichen in Verbindung gesetzt und gesagt, okay, bevor du live gehst, brauchst du ein Berechtigungskonzept, weil das Berechtigungskonzept für uns ist die Grundlage, um im Optimalfall automatisiert zu onboarden. Ein Onboarding von Anwendungen ist aus meiner Sicht relativ einfach, wenn man eine saubere Datenstruktur oder Berechtigungskonzept hat, was maschinell auslesbar ist. Weil dann kann man relativ einfach über eine CSV-Schnittstelle Berechtigungselemente in einem IAM-System erzeugen. Die Personaldaten kommen sowieso seitens HR. Dann ist man erstmal im IAM-System. Dann ist die Frage der Strategie, wollen wir ein manuelles Provisioning oder Deprovisioning oder wollen wir ein automatisches? Eigentlich will man immer automatisch, aber oft ist das Thema mit Kosten nutzen nicht gegeben, dass wir immer automatische Schnittstellen implementieren. Deswegen kann es auch sein, dass man dabei bleibt und sagt, wir haben einen Benutzeradministrator, der selbst Aufträge vom IAM-System im Zielsystem umsetzt. Offboarding aus meiner Sicht ist auch relativ simpel. Da reicht ein periodischer Abgleich gegen das IT-Asset-Management-System, welches auch immer es ist. Die meisten Unternehmen haben irgendeine Art ein System, wo IT-Assets gepflegt werden, eine CMDB oder ähnliches. Wenn dort zum Beispiel irgendwas steht mit End of Life oder Deprovision, dann kann man entweder manuell oder automatisiert abgleichen und sagen, diese Anwendung geht End of Life bis X. Bis zu diesem Zeitpunkt, vielleicht möchte ich noch eine grace period definieren, aber nach diesem Zeitpunkt schmeiße ich alle meine Berechtigungselemente inklusive der Information über die

Anwendung aus meinem IAM-System raus. Das heißt, schnelle standardisierte Prozesse fürs Onboarding, nämlich zum Beispiel ich habe ein Template, in dem ich hochlade, dann das Einbetten der Prozesse oder der IAM-Trigger in das Application Life-Cycle des Unternehmens und periodische Abgleiche mit dem IT-Asset-Management-System des Offboarding. Für mich, das Incident Management und das IAM greift nur bedingt ineinander.

Wo man eine große Überschneidung hat, das ist beim Thema Privilege Access Management und Incident Management, das ist eng verknüpft. Wenn du Privilege Access Management als Teil des IAM verstehst, dann hat die Auswirkungen. Das hat weniger mit den Userzahlen zu tun oder dem On- und Offboarding von Personen, sondern eher über den Fall, wie identifiziere ich ein Incident? Das ist zum Teil PAM. Incidents werden häufig dadurch erzielt oder gefördert, dass Leute zu viele Rechte haben und mit ihren Rechten kritische oder privilegierte Handlungen vornehmen können, die schädlich sind für das Unternehmen. Im Bereich Privilege Access Management machst du diese Handlungen erst mal sichtbar. Wenn du jetzt den IAM-Kosmos nicht verlassen möchtest, dann bist du hier am Ende. Dann hast du gesagt, ich habe Privilege Access Management, das hat funktioniert oder das hat nicht funktioniert. Mein Privilege Access Management Tool, was meistens in Nutzung ist, sagt mir sogar, hier ist ein potenzieller Incident oder es gibt Daten, aus denen ich potenzielle Incidents herauslesen könnte. Wenn wir dann keine fachliche, funktionale und organisatorische Schnittstelle ins Incident Management haben, passiert nichts. Das heißt, das Thema IAM kommt dann ins Spiel und das ist für mich Teil des Incident Managements. Aber aus meiner Sicht hat das On- und Offboarding von Anwendungen bezüglich Incident Management noch keine großen Zusammenhänge, außer du gibst mir einen.

I: Wie unterscheidet sich die Verwaltung von Usern in IAM-Services von der in anderen IT-Services?

A: Dass wir die Services und die Userverwaltung und die Prozesse hinter der Userverwaltung wirklich so gestalten, dass es der User am Ende nichts mitbekommt. Also ich glaube, IAM ist einer der wenigen Services, wo wir nicht wollen, dass Leute großartig mitbekommen, was im Hintergrund passiert. Wie gesagt, also das beste IAM funktioniert lautlos. Eine Sache vielleicht, die Schwierigkeit bei dem Thema IAM zusätzlich ist noch und auch das hebt sich ab von vielen anderen Services. Wir haben immer, wenn du zum Beispiel einen Application Verantwortlichen nimmst, der verantwortet eine Applikation, dann ist diese Person für das Unternehmen eingestellt worden, um diese Anwendung zu verwalten. Mit dem IAM-Thema kommen wir jetzt um die Ecke und erklären dieser Person, dass er über seine normale Tätigkeit hinaus noch ganz viel für uns machen muss auch,das heißt, , viele Mitarbeiter, die auch vielleicht gar nicht so technisch versiert sind, sind auf einmal mit technischen Themen konfrontiert, mit denen sie gar nicht konfrontiert sein wollen. Dafür wurden sie auch nie eingestellt. Aber sie müssen sich aufgrund meistens irgendwelchen Governance-Vorgaben dem unterwerfen. Das heißt, wir haben auch sehr viel aufgrund der Natur oder der Sache mit sehr viel Ablehnung zu tun innerhalb des Unternehmens bezüglich dem Service IAM. Und das muss man adressieren auf unterschiedlichste Art und Weise.

I: Welche Strategien würden Sie einsetzen, um die Skalierbarkeit von IAM-Diensten zu gewährleisten?

A: Ehrlicherweise hatten wir auf allen Projekten bisher die Schwierigkeit der Skalierbarkeit. Das eine ist einfach die technische Schwierigkeit der Skalierbarkeit der eingesetzten Tools. Auch Tools haben Grenzen in ihrer Schnelligkeit von Berechnungen. Je mehr Daten ich da reinwerfe, desto langsamer wird es. Ich weiß nicht, ob das in der Zwischenzeit besser geworden ist. Wir sind auch bei sehr großen Unternehmen unterwegs, fairerweise, aber auch je größer das Unternehmen, je umfangreicher die IT-Landschaft und desto umfangreicher auch die Berechtigungsstruktur, desto schwerer wird es für ein System auch beispielsweise in Echtzeit zu handeln. Das muss teilweise passieren. Im Kontext SOD zum Beispiel, dort Ergebnisse zu reduzieren. Was ich aber plädiere, was jetzt nicht technisch ist, ist das Thema, wir wollen die Prozesse so einfach halten wie möglich. Weil, wenn du dich auf die Kernprozesse

im IAM konzentrierst, müssen die nicht komplex sein. Die werden immer erst dann komplex, wenn wir anfangen, oder auch wenn der Kunde anfängt, Sonderlocken mit einzuweben. Jeden Fall, also auch jede Abweichung, die kommen könnte, prozessual schon abzufangen. Da bin ich gar kein Fan von. Die Prozesse sollten so einfach wie möglich sein. Wenn Sachverhalte in diesen einfachen Prozessen nicht händelbar sind, dann ist es aber auch eine Abweichung des Standardprozesses. Da muss man sich eher überlegen, was passiert mit dem Rest. Aber im Standard wollen wir so einfach wie möglich sein. Das heißt, kein Abbilden von Befindlichkeiten einzelner Personen oder von politischen Konstrukten. Auch kein Abbilden irgendwelcher Sonderlocken. Der letzte Punkt ist, so viel automatisieren wie nur möglich. Das heißt, weg von der manuellen Benutzeradministration hin zu automatisierten Schnittstellen und die müssen einfach technisch gebaut werden.

I: Wie gehen Sie mit variablen Userlasten um und welche Rolle spielt die flexible Ressourcenzuweisung in diesem Zusammenhang?

A: Ich weiß aber nicht, ob dir meine Antwort gefällt jetzt. Ich bin aber der Meinung, dass wir gar keine so hohe Varianz in dem IAM-Thema haben. Weil die Berechtigung, es gibt unterschiedliche Orte, wo Varianzen auftreten können, oder wo Dynamik reinkommt. Der eine Punkt ist Berechtigungsstruktur. Das Einzige, was du hast, es kommt mal ein System dazu, es kommt mal ein System weg, ist das aber von der Menge, aus meiner Sicht, nicht ausreichend, um jetzt hier groß mit, wie hast du es genannt, elastic resource allocation zu spielen. Ich glaube, das was da an Varianz da ist, kann jedes System mehr oder weniger berechnen. Wir haben eigentlich auch keine große Varianz beim Thema der Userzuweisung. Wer darf was? Du hast natürlich an Stichtagen , Abteilungswechsenl, mehr Anfragen für neue Rechte oder dem Löschen von alten Rechtenzuweisungen als an anderen Tagen. Aber auch da solltest du eigentlich keine große Varianz haben. Für mich persönlich, wenn du eine große Varianz hast im Bereich IAM, dann können das nur zwei Themen sein. Entweder du hast eine organizationstechnische Reorganisierung, also dass sich das Unternehmen reorganisiert, Abteilungen werden umgezogen und inhaltliche Aufgaben werden umgezogen. Dann hast du eine Varianz, die ist auch erklärbar und der zweite Teil ist entweder ein Fehler oder ein Incident. Wir haben in der Vergangenheit auch solche Varianzen so behandelt. Wir haben Prozesse gebaut, wo wir Thresholds angelegt haben, wo wir gesagt haben, wenn wir von HR mehr als x Datensätze bekommen oder zum Beispiel für die Anlage von Usern, aber noch viel schlimmer für die Löschung von Usern, dann verarbeiten wir die erstmal nicht weil diese sind untypisch und müssen wir uns erstmal genauer anschauen. Das heißt, wir haben eigentlich zum Thema Varianz eher damit gearbeitet, wenn wir eine zu hohe Varianz haben, stimmt hier irgendwas nicht. Auf der anderen Seite habe ich ja zuvor gesagt, und das passt aus meiner Sicht dennoch zusammen, dass wir eine sehr hohe Rechenlast haben können. Das stimmt schon, aber die ist tendenziell sehr hoch und die ist immer sehr hoch. Das muss man sich nur vorher bewusst machen. Zum Beispiel im Kontext SOD, wenn ich dort eine Methologie baue, die sehr komplexe Berechnungen erfordert, dann füge ich die einmal ein, dann habe ich gegebenenfalls einen höheren Bedarf an Rechenleistung, aber den habe ich immer. Also ich bin der Meinung, wir haben eigentlich keine große Varianz, und wenn wir eine haben, dann deutet das darauf hin, dass es entweder organisatorische Veränderungen gibt, Fehler oder tatsächlich auch Incidents.

I: Wie definieren Sie 'hohe Effektivität im Kontext des Availabilitymanagement für IAM-Services?

A: Da würde ich getrennt antworten, weil da gibt es für mich einen Riesenunterschied zwischen IAM und PAM. Bei IAM muss aus meiner Sicht die Availability nicht wirklich hoch sein. Da reichen mir 90 Prozent, 80 Prozent. Wenn dein IAM-System down ist, können trotzdem alle arbeiten. Das Einzige, was in der Zeit nicht passieren kann, ist, dass ein Mitarbeiter ein neues Recht bekommt, was er vorher nicht hatte. Und selbst das kann er im Zweifel, wenn das IAM-System down ist, sich direkt im Zielsystem holen, über einen Sonderprozess, über manuelle Menschen, die sagen, okay, wir verstehen, hier gibt

es irgendwas, du musst da unbedingt dran. Ganz anders als bei einem PAM-System. PAM-Systeme müssen hoch verfügbar sein. Zum Beispiel CyberArk und so ist auch die Lösung von CyberArk. CyberArk ist Marktführer im Bereich PAM. Die Lösung von CyberArk ist so aufgebaut, dass es auch geografisches Mirroring gibt der relevanten Komponenten, sage ich jetzt mal. Warum? Weil an CyberArk oder an ein PAM-Tool binden wir all die Assets an, die superkritisch sind fürs Unternehmen sind. Das heißt, wenn die down sind, hat das Unternehmen echt ein Problem. Wenn mein PAM down ist, ist das auch noch nicht so schlimm, weil ich kann normalerweise auf anderen Wegen noch in meinem Asset arbeiten. Schlimm ist, wenn beides down ist. Mein Asset, was ich bearbeiten möchte, ist down. Ich möchte es über PAM fixen. Kann ich aber nicht, weil PAM auch down ist. Das ging schon so weit bei einem Kunden. Die hatten so ein schlechtes Bauchgefühl bezüglich der Availability ihres PAM-Systems, dass wir einen manuellen organisatorischen Prozess gebaut haben, der physische Tresore beinhaltete und Menschen, die angerufen werden, wenn etwas passiert. Einfach nur für den Fall, dass die Systeme nicht erreichbar sind. Dann haben wir einen Pen-and-Paper-Prozess designt, um dies sicherzustellen und mit Personen, die auch 24-7 erreichbar sind. Das ist dann das nächste. Um sicherzustellen, dass zu jeder Zeit, vielleicht mit ein bisschen Verzug, egal ob die IT da ist oder nicht, jemand privilegiert handeln kann in deren wichtigsten Kernbanksystem, das war eine Bank. Wenn du Authentifizierung mit reinzählst, würde ich meine Antwort revidieren und sagen, da muss ebenfalls eine hohe Availability hergestellt werden, weil sonst kann keiner arbeiten. Wenn du jetzt von einem zentralen IGA-Tool, so nennen die sich ja meistens, also Identity Governance and Administration Tool, wenn du nur davon ausgehst, weil ein Authentication Provider, der macht nichts anderes, außer zu sagen, Manuel ist Manuel, der kann da rein. Und der kann aber dann nur da rein, wenn vorher ein IGA-Tool nicht geregelt hat, was Manuel da drin darf. Also Authentication Services Availability sehr hoch, IGA-Tool nicht so hoch, PAM-Tool sehr hoch.

I: Welche spezifischen Mechanismen würden Sie einsetzen, um die Kontinuität für IAM-Services zu gewährleisten?

A: Ehrlicherweise, um die Kontinuität von IAM-Services sicherzustellen, da unterscheidet sich IAM nicht von anderen wichtigen Services in Unternehmen. Was meine ich damit? Es gibt wieder Ablaufpläne im Sinne von Disaster Recovery, die vorher definiert werden müssen. Es müssen regelmäßig Backups definiert werden. Es muss sich darüber Gedanken gemacht werden, wie wird gelöscht oder wird überhaupt gelöscht. Also die klassischen BCM-Themen und IT SCM-Themen, die unterscheiden sich nicht von anderen wichtigen Services, nur weil es in IAM-Services aus meiner Sicht. Es gibt im IT-Asset-Management ja meistens IT-Assets die gemäß Kritikalität eingestuft werdenuUnd wenn der IAM-Service, das machen nicht alle Unternehmen, aber wenn der hoch eingestuft ist, dann gelten für den genau dieselben Anforderungen im Sinne von Disaster Recovery und Backup und Incidence Response wie für alle anderen wichtigen Assets auch, was auch immer dein Unternehmen ist. Wenn es eine Bank ist, machen wir das Gleiche, was ein Kernbanksystem auch machen muss. Ich glaube, da gibt es keine große Unterscheidung. Da ist eher die Frage, da müsstest du jemanden fragen, aus dem sein Kerngebiet BCM und IT SCM oder Incidence Response ist, was er der Meinung ist, was High Critical Assets für ihn erfüllen müssen im Sinne der Kontinuität.

I: Wie wird Modularität im Servicedesign von IAM-Diensten implementiert, um den vielfältigen Bedürfnissen der Kunden gerecht zu werden?

A: Ich würde das Thema IAM sachlich schneiden. Und zwar in einzelne Pakete tatsächlich. Und würde dann, und so machen wir es ehrlicherweise auch, nicht nur, wenn die Applikation Kunde des Services ist, sondern auch wenn der Kunde uns anfragt. Ehrlicherweise, ich würde es gleich behandeln. Ich würde sagen, wir haben einen IAM Service, der beinhaltet erstmal alles. Und du kannst jetzt einzelne Pakete auswählen, die du von uns unterstützt haben möchtest. Beispiel, Authentifizierung, also hast du es vorhin selber ja schon gesagt, Authentication ist ein Teil. Für mich einigermaßen ein kleiner Teil, weil

dafür gibt es Lösungen. Das ist nicht wahnsinnig schwer zu implementieren. Da musst du nur einheitlich über das Unternehmen sein. Viel schwieriger ist alles rund ums Access Management. Weil da gehört Role Management dazu, die Vergabeprozesse dazu. Dann kann man sich dem Thema Account Management widmen. Ich kann dir gleich die Sachen mal definieren, wie ich es machen würde. Ich würde ein Service Portfolio bauen und würde sagen, wir liefern dir Identity Management, wir liefern dir Access Management, wir liefern dir Account Management, wir liefern dir Kontrollen. Mit Kontrollen meine ich SOD Methodiken, Prozesse, wie das anzuwenden ist, Reconciliation, also SOD Listabgleich zwischen IAM-System und Zielsystem, Access Reviews, brauchst du Hilfe bei Access Reviews, brauchst du Hilfe bei Privilege Access Management, brauchst du vielleicht sogar Ersthilfe in deinem Bereich IT Service Management, kennst du überhaupt deinen Scope als Kunde. Dann würde ich, für all diese Themen einen Standardprozess bauen und würde den auch implementieren und würde dann den Anwendungen und den Anwendungsverantwortlichen anbieten, zu sagen, wenn du diesen Service nutzt, so wie wir ihn dir vorgeben, dafür musst du dich vielleicht verbiegen, aber wenn du das machst, dann bist du auf einen schlag Compliant und wir haben sie super effizient gebaut. Langfristig gewinnst du damit. So würde ich es machen.

I: Können Sie ein Beispiel dafür geben, wie Modularität in IAM-Services die Dienstleistung für interne und externe Kunden beeinflusst?

A: Ich glaube, wenn du ein modulares Service Portfolio baust und dem Kunden in Anführungszeichen die Wahl lässt, was er nutzt, dann kriegst du nie eine richtige Zentralität hin und eine Einheitlichkeit über alles, weil sich dann jeder das rauspickt, was für ihn am einfachsten und im Zweifel auch am günstigsten ist. Das heißt, du müsstest, wenn du den Weg, weil das fehlt eigentlich in der Frage aus meiner Sicht, damit das funktioniert, wenn du den Weg des Service-Pakete gehst, dann brauchst du auf der einen Seite aber eine Governance, die relativ viel vorgibt zu diesen einzelnen Service-Paketen, weil sonst baust du dir durch das Schneiden des Services eine sehr dezentrale und ungleiche Welt und das möchtest du im Normalfall im Bereich IAM nicht haben. Die Unterscheidung zwischen intern und extern, verstehe ich zwar, macht aber für mich keinen Unterschied im Prozess und in der Technik.

I: Inwieweit erfordern IAM-Services eine höhere Integrationsebene mit anderen Unternehmenssystemen?

A: Auf meinem Zettel steht wesentlich, als ich mir das vorüberlegt habe. Warum? Weil das IAM-System aus meiner Sicht nimmt eine zentrale Rolle ein im steuern des Unternehmens. In der Effizienzsteuerung, wenn Leute immer Monate, Wochen auf ihre Rechte warten, das beeinflusst die Effizienz des Unternehmens im negativen Sinne. Aber das IAM-System ist nicht immer führend für alle Informationen. Zum Beispiel das IAM-System ist im großen Stil darauf angewiesen, dass die Daten, die aus HR kommen richtig sind. Das IAM-System ist nicht führend für Personaldaten. Personaldaten kommen aus einem oder mehreren HR-System immer und wenn die schlecht sind, kann ich auch nie ein gutes IAM-System bauen. Auf der anderen Seite ist es wichtig, dass wir eine hohe Automatisierung in unsere Zielsysteme haben und es ist auch wichtig, dass wir aus IAM-Seite Daten so bereitstellen können, dass wir als Provider für andere Services dienen können, wenn notwendig. Zum Beispiel für ein Azure Active Directory oder für irgendwelche Group Directories, die es meistens gibt. Das heißt, auch wir können Informationen weiterleiten die wir bekommen. Beispielsweise das IAM-HR-System werden bei uns angereichert, für Zuweisungen von Berechtigungen, für weitere Metadaten, die gegebenenfalls vorher nicht erfasst wurden und es kann sein, dass Anwendungen oder weitere Services diese Daten von unsererseits brauchen. Dann müssen wir natürlich versuchen, Endpoints bereitzustellen, sodass man die möglichst standardisiert auch abgreifen kann über REST APIs oder sonstiges.

I: Wie priorisieren Sie Interoperabilität und standardisierte Protokolle im Kontext von IAM-Services?

A: Ich kann dir sagen, dass wir bei diversen Kunden auch schon ein Problem hatten bei der Interoperabilität innerhalb des IAM-Systems, weil du hast zum Beispiel auf der einen Seite ein Provisioning Engine, auf der anderen Seite hast du eine Datenbank. Dann hast du so eine Art Ticketing-Komponente oder Modul innerhalb des IAM-Systems, wo du jedenfalls Prozesse abbildest und wenn das nicht funktioniert, das Zusammenspiel dieser Komponenten, dann hast du sowieso schon verloren und an sich bin ich großer Fan von Standardisieren, wo es nur möglich ist. Und zur Not auch Software, die mit diesen Standardprotokollen nicht umgehen können, nicht einkaufen, das würde ich knallhart so machen.

I: Interviewabschluss: Gibt es von Ihrer Seite aus Punkte, die noch nicht angesprochen wurden, die Sie aber hinzufügen möchten?

A: Von meiner Seite passt alle.

I: Ich danke Ihnen aufrichtig für Ihre Bereitschaft und die Zeit, die Sie sich genommen haben, um ein Interview mit mir zu führen. Sollten Sie an den Ergebnissen meiner Bachelorarbeit interessiert sein, werde ich Sie im September darauf ansprechen und sie Ihnen präsentieren.

Appendix 7: Interview Transcript V

General Data:

Interview-Type	**MS-Teams**
Interview-Number	**5**
Interview Date	**01.08.2024**
Interview-Duration (in Minutes)	

Demographic Data:

Industrial Sector	**Insurance**
Role	**Service Manager/Lead**
Experience in IAM / ITSM (in Years)	**3**

I: Thank you for taking the time to conduct an interview with me as an expert today. Before we start the interview, I would like to briefly introduce myself and give you some information about me. My name is Manuel Yambao and I am in the final stages of my Business Information Technology bachelor's degree at the University for applied Science Ulm and University for applied Science Neu-Ulm.

As part of the interview, I would like to ask you some questions regarding ITSM and IAM services. If you agree to this, please confirm briefly. If you have no questions, I would now like to start the interview. Otherwise, we can clarify any open questions you may have beforehand.

I: At the beginning of the interview, please tell me about the general tasks you perform in your company.

A: I'm currently Service Lead for the CIAM Product of a reinsurance company.

I would say in CIAM, specifically my roles include managing customers who have basically their feet and hands dug deep into CIAM, which is the identity provider for end customers, which is a global product that is being used technically for authorization of clients to reach the reinsurance platforms or company associated platforms.

Short about also what I've done in the past, I was also the service lead for APIM, which is the API management platform used by a lot of company associates and company internal products.

There I was also a service lead and I was responsible for managing similar aspects like managing the operations, including the publishers of APIM and also the demands from the publishers, translating them to the APIM team so that these demands could be then implemented in the productions. Coming back to CIAM, this is what I do as well. I take over the demands from different associates and partners. Major partners are basically all over the globe, but they are majorly in the US and the UK, where we take in the requests.

But these requests are also in the Southeast Asia region. Recently we've seen a spike in the Southeast Asia region and US region where we're doing a lot of federation requests. We're doing the user lifecycle management for CIAM.

We're doing the access controls. We're doing the authentication and authorization through multiple ways and the centralized management. I would say there are two platforms that our company uses. One is IAM, which is the identity and access management, which is technically for all the accesses related to the internal customers, the initial accesses that one might need. So, let's say a cloud account. The credentials related to the cloud account; the accreditations related to the cloud account are managed over IAM. CIAM is technically just for authorization concepts for external customers. This would not mean that we do not do anything for the internal customers. We do provide them accesses, but for that they have to go through a layer of IAM, which is internal to the company usually.

I: What characteristics does an IAM service have that distinguishes it from other IT services?

A: CIAM could be just the authorization layer. Obviously it has to be compliant. It has to incorporate all the risks and make sure that the risks are tackled.

This is just an authorization concept. For other risk assessments, for other compliance related software, for other tools that people might use, there are different aspects to it.

For example, for a risk assessment software, you might have to give a risk score to it, which CIAM doesn't provide.

Or for compliance related software, you might have to tell at the end of the day, what are the different assessments that you did for compliance?

So different levels of assessments that you did probably relate to the services, descriptions, also related to the access identified.

So CIAM becomes a part of it inherently. CIAM just plays a role in technically all of this software of just providing an authentication and authorization mechanism for end users.

So CIAM has to make sure that if the external users are logged in to a company domain, that they do it in a compliant way and in a non-risky way specifically.

So that is what CIAM plays as a role. It plays a part of it. It necessarily doesn't have to stay your way. Some customers might incorporate so it’s an optional tool that the customers might incorporate. Some do not. Some use Microsoft 365 tools for doing that.

CIAM uses Azure B2C, for example, in that case. So that is the major differentiation, I would say. So there are different other ways of doing the authentication and authorization.

CIAM just provides a platform to do that through Azure B2C.

I: Can you provide examples of how IAM services respond to frequent application onboarding and off-boarding processes?

A: Okay, so I mean as a part of on boarding, I would say the customers usually ask for self-service as the central aspect. They should be able to manage their user base. I would say CIAM, in context of CIAM, keeping it in context of CIAM itself, there are a couple of self services portals that we offer to the customers or internal customers or external customers which we use. But obviously self service portals doesn't necessarily mean that the backend is sorted. So, for the backend on boardings, obviously based on the use case, there might be different requirements from the customers that might come in. I would say example here would be a customer from the US who has currently their portal for onboarding a customer, but they would like to integrate CIAM because they want to move away from one type of solution or they want to have a hybridized solution. In that case, we have to develop different policy based access management. In case of policy based access management, what we do is we just create a policy for them saying how the access flow would look like, how the role authentication would look like in that access flow, and if that would be a single sign on or if that would be a local login.

Based on these logins, we have auditing scenarios. We provide last login timestamps that we make sure that the customers are able to see we perform an account lifecycle for a user, making sure that the user is deregistered from that application or from CIAM after a specific amount of time.

Moving towards, you know, that would pave our path to the offboarding scenarios, users usually are deregistered or deactivated from CIAM platforms after a specific amount of time as a part of account lifecycle, but the application offboarding for us would mean that we go ahead and we deregister the user, deregister the roles that the user has.

Make sure that if the application is using a CIAM API endpoint, we deregister that. And based on that, we finish off all the offboarding scenarios. We've got like 10 to 15 controls that we have for offboarding, which we have to complete before we finish off the complete off.

You know, we say that the offboarding is done.

Regarding the amount of users this could mean, if you're talking about quantitatively, you know, what CIAM technically has to offer in that case, the possibility is technically limitless. We do not set any limit on the amount of users that needs to be onboarded.

Since it's a self-service mechanism, the users can be onboarded, you know, through a bulk invitation mechanism, or they could just automatically federate to our or just use an automatic onboarding mechanism. I wouldn't put a number to it. I would say that until now we federated customers to us with multiple email domains, because, you know, 10 to 15 email domains, and now we're working on 2,000s of email domains that we're federating, which means you can scale it up to a number, like yourself, saying that if there is a domain, and there are thousands of users to a domain, it would add up to millions and then also to billions at the end.

I: How does the management of user identities in IAM services differ from that in other IT ser-vices?

A: There are different scenarios that you should consider in this aspect, according to me. One would be an SSO scenario and one would be a local login scenario, right?

In terms of SSO, I would consider this as some kind of advanced authentication, I would say, where we use SSO, but we make sure that there is a multifactor authentication associated to it.

There is another aspect to it that the users, I mean, for a user who's logging into SIAM or into a SIAM portal, associated portal, would see usually an option based on how the application is set up.

If the application allows them an SSO, they would be able to use an SSO, otherwise they would have to create a local login which basically asks them to create a password for themselves.

A user can identify in both ways or in a hybridized way, however the user would like it to be.

CIAM in terms of that would be a flexible tool, I would say, which provides users both or all the three options and a glance.

You have to also understand that this is as granular as it can go. This is the most granular form.

User can reset a password, user can reset their MFAs, nowadays the user can also have a centralized mechanism, so the admins can manage the users.

Attaching to the fact that users also have a specific user lifecycle that is running in the background, which makes sure that the user who's logging in has a timestamp to it and this is being recorded.

For a user, usually, what matters is to make it easy and accessible, everything that we're doing.

An IAM service, in that case, according to me, should incorporate all the three that CIAM is also providing and above and beyond be compliant and make sure that there are,

that the user information is bundled and the user feels secure while logging in. That is what I would see as IAM service from a user perspective.

If comparing the differences and the nuances, I would say would be too big.

Every product nowadays uses MFA, for example, so CIAM uses MFA as well.

The nuance here would be CIAM currently is not an app-based MFA.

It is just a feature which we will be using in the future, but currently not.

The others are already using an app-based MFA. That would be one difference that I can think on top of my head. The other difference is an SSO integration that CIAM provides, which is, I would say, a unique proposition that we have in terms of CIAM that we do SSOs. The other customers really don't do the SSOs in that way.

I: What strategies do you employ to ensure the scalability of IAM services?

A: We are lacking on the rapid recovery part. I mean, obviously, we have the failover Plan in general. We have a failover mechanism but it is a switch based mechanism. It is not automated. A lot of things in CIAM really are not yet automated. For example, the effective also includes how quick the users are boarded or how quick these things are happening. We are not that quick. The Operations team, which I am leading right now, does that really manually. We are missing that automation right now in a way of the onboarding, for example, the app registrations would be done automatically. The self service portals will then be more usable. Third would be then making sure that the customers are also aware about the rapid recovery. Let’s say if the customer requires that the traffic moves from one region to the other, we provide them the rapid recovery, which is an automated scenario. Currently, this is a very manually done scenario. That would be the next steps that science has to tackle.

I: How do you handle variable user loads, and what role does elastic resource allocation play in this context?"

A: For variable user loads, there are different parts to it. From the hardware context, obviously you do some kind of load balancing. The instance that we're using in Azure B2C is some kind of load balancing in terms of regions. If a region fails, there is a turnover that the traffic can be diverted to another region. Similarly, to make it a bit more live, you know, there are admins who are using the user management tools. For them as well, it is important to make sure that this is live and the best way to make it live is

using a cloud mechanism. Because cloud provides you the scalability, cloud provides you the live ability, the computing power needed for it and also the associated mechanisms, for example, something like the last load logon would be a caching mechanism. A cloud system would provide you a best use case for it and reduces the latency as well. That is what I think we provide as a USP to the customer saying that we are live. You can check the information at all times. If the system is down, there is some kind of load balancing that kicks in and beyond, above and beyond that. I mean, we are not there yet, but we're using some kind of observability tools, for example, data dog. In that case, it manages the alerts and also monitors the whole scenario for us. We can see how, let's say, a CIAM API is performing at a given point of time. If the performance is optimal or if it is not.

I give you a very concrete example. We had an outage recently where we found out that we're using an endpoint from I mean, which is a redirected endpoint, API endpoint. We then decided, I mean, we already had a fall over of Azure website based endpoint, which is a direct Azure endpoint and we could directly within like one hour or two hours, we could get the users back online. I think it was just less than one hour that we got the users online based on the fall over that we had. We just had to click on a switch and that would fall over. We are now making sure that these endpoints are scalable as well. Because the problems that we had in the past were also shown to us by the monitoring and alerts that we had in science. We are making sure that we tackle those issues. We have tackled them now and we're making sure that this is resolved in the future. This is also the scaling mechanism that comes with it.

I: How do you define 'high effectiveness' in the context of availability management for IAM services?

A: So for me, load balancing, I would start with the stability, right? Stability incorporates load balancing, rapid recovery scenarios, reliability, in terms of, you know, the UI as well. At the end of the day, making sure that it is a consistent UI. The UI is up all the time. We don't have any failovers there or problems there. All these things account to the effectiveness, I would say, of a system and in terms of availability management, so coming to an ITIL perspective, availability management in ITIL is technically, you see, if all the systems are up, how long has it been up? If there has been a downtime, how long was the downtime?This would give you a matrix, how long can you keep your systems up and you can provide an SLA at the end of the day saying it's a 99.9%, 98% or 90%. You can put a number or a label to it. How much availability can we provide you? Keeping that aspect into mind, I think you have to make sure that your monitoring and alerts mechanism is also working. The best case, I would say, would be to have an observability, which ITIL, for example, doesn't incorporate right now. But observability is, I think, where the users or the systems want to head to. The systems engineers and everybody wants some kind of observability. They want a proactive mechanism instead of a reactive mechanism in that case. This is what I think what matters to the availability management and effectiveness. You should be proactive in finding out what could lead to a fallback and you should be able to manage before time rather than just in time.

I: What specific mechanisms do you implement to ensure service continuity for IAM services?

A: So, I mean, observability is good to have. I mean, it's something that is developing in the past. But what's not developed right now is, for example, a lot of the customers that we see don't have a disaster recovery plan and they're really reliable on us and for our disaster recovery. So that is the reactive part of it. The security measures that we take in place with the disaster recovery. We do a disaster recovery every year. We check what would happen in case, you know, everything is down. But I mean, we're good in that aspect. But what's missing, according to me, is people forget that there is, with disaster recovery, with the security measures in place, they have to keep something on their end as well that they have as a hybrid isolation. There should be an alternative mechanism on the application end as well, which would be good to have, I think, for the customers. I mean, it costs a lot, but still, you never know. You might take that.

I: How is modularity implemented in the service design of IAM services to meet the diverse needs of customers?

A: The best case, I would say, is I would take an example of a federation request. A federation request is the most complicated request that a customer provides to us because this has approximately, if I'm not wrong, 15 to 20 fields minimum that the customer should provide us, where we have to show the flexibility or the modularity in our situation. Now to tackle those requests, we have different scenarios. Obviously, we do provide a standard scenario to the customer saying, hey, probably you don't have experience with the field. We review a standard scenario. You can use the standard SSO and use it the way it is, which incorporates both federated SSO login, hybrid login, local login, all of it. But then again, there are customers who want it to be optimized to their application, to their product. A good example would be an American client right now who wants to manage with both Microsoft 365 and Azure B2C, making sure that there is some kind of redundancy. Now this includes some kind of extensions that we have to incorporate in our system. And a best example would be that we have to then create a policy, a custom policy for them. We have currently about four to five customers who have these needs, these necessities, where we develop custom policies for these customers. Above and beyond, we do have a positioning of a custom API. We do provide customers an API endpoint, which they might use to manage the database inside, but just have it done through an API, which gives them the possibility to use all the same functionalities, to leverage all of them on their platform with having their own faces but having sign in the background doing all the services for them. Similarly, the custom policies in that way also do the same thing. But in that case as well, we do provide some kind of sign in branding. The user interface in that case would see some kind of sign branding or something which is file specific and the look and feel of it is also playing a rather massive role because the customers want to see, for example, I had a meeting with the customer yesterday. They came to us asking for situations where they don't want to even validate the customer's first name and last name because they're sure that what the customer is providing is correct. We have to say in that case, yeah, all right, this is possible, or this is not possible. Obviously, we stay flexible. But this is something that falls under the whole scope of policies. We change that in the policies. We do the deployments accordingly. We make sure that there are hybridized deployments, right? As I said, because the customer has a different user base, and we use a different backend. Customer uses Microsoft 365 Dynamics. We use the OVTC provider. A customer might use Entra, another might use Octa and so on. We make sure we incorporate it through the policies that we have. We provide them custom policies. We provide them API endpoints. We provide them different types of plugins. We make sure that there is a MFA. We make sure that we adapt it to the customer needs. If the customer just needs a phone-based MFA, SMS-based MFA, app-based, the customer should be able to select what they need and similarly, in terms of the user interface as well. All these parameters, I would say, would account to the modularity.

I: Can you give an example of how modularity in IAM services affects service provision for internal and external customers?"

A: So technically, a person would expect that the standard policy or the standard solution that we provide to the customers, would suffice at least if not all the internal customers. So that would mean that we see a lot of customers saying internally as well that you cannot fix to a standard. We hear this a couple of times. We expect this from an external customer, definitely. At any given day, we expect this from an external customer because they are not part of this organization. But a customer or a product coming from internal to the organization, we somehow inherently expect that the standard solution would suffice. Which is not the case. We see deviations from the standard solution also to the internal customers. A very good example here would be: We have a customer who is tackling risk assessments. They just want to make sure that the customer who is coming in has another layer of authentication. I mean,

there's MFA, definitely, but they do a role-based authentication as well. And this role-based authentication is done on their system, which would mean that the style of the solution doesn't encompass what they need. Therefore you see that this part, specifically the role-based access control that we have for the customers, usually differs based on the usage. You cannot really generalize. You cannot standardize in that way. You have to stay flexible. You have to propose this modularity concept to all the customers, be it on the internal or on the external. Now, talking about an external customer, I want to give you a concrete example. For an external customer, they deviate from the standard solution by providing them even with the social IDPs. You have Google, Facebook, LinkedIn for them, which we don't use for the internal customers. We don't even propose to the internal customers because the compliance comes into play for those decisions. Now, the organization for these internal modularities, we can make sure that we educate the customer. We tell the customer that this is not compliant. The security policies don't allow us to do that. Thereby, we don't propose that to the customers internally as a solution. But for the external customers, we make sure that we can add a security layer to it because they are obviously managed majorly on the external. And we're the ones who are just creating like a small piece of it, providing them the back end to it. But that's just one token that we provide to the customer saying, hey, that's the authorization. Take it or leave it. So that is the difference that you see at the end of the day within the internal and external.

I: To what extent do IAM services require a higher level of integration with other enterprise systems?

A: Basically, an IAM system should provide according to me in terms of higher level of integration. One thing is, let's say we need to facilitate SSO. There is a key ecosystem where the customer comes and wants to have a login and doesn't want to enter multiple passwords. Doesn't have to remember multiple passwords. Doesn't have to have that role authorization. Doesn't have to provide his role to it. I would say the SSO integration plays a very big role in that case, in those levels of integrations. The other part would be to have a very reliable database at the back end. Now this database, what we use is based on the Azure B2C services. We use that as we consider that to be really reliable. Where we are ensuring a consistent enforcement of our policies. Basically, security policies, we make sure that every security policy that the customer expects from us is provided through these databases. Can I name it a centralized platform? This shouldn't be that segregated. I mean, the customer can have some kind of fallback scenario for themselves, but we should be the centralized platform. Providing both the options that the customer needs and also the security policies that we need to implement. There are controls that we should be able to present. I would say it is a centralized control that we can set at the end of the day. Above and beyond, it is very important to be compliant. To have user lifecycle being done on a regular basis. To make sure that there is some kind of account provisioning and deprovisioning system that adapts to the changing mechanism. If a user leaves the organization, the user should not be entitled for that role as well. Therefore, the deprovisioning in that case plays a big role. Then at the end of the day, there is office of the, not CIAM, but SIEM system. You know the SIEM system. The Security Information and Event Management, it is called. All these, we should make sure that this is in place. This SIEM system is in place and definitely for each user, including incorporating it into the security mechanism. That would also mean the multi-factor authentication. Making sure that there is not just one layer, but multiple layers checking that the user is authorized. And which currently lacks, I would say, coming back to the observability point, would be understanding the risks and making sure that there is some kind of intelligence in that way as well. Making sure that there are some kind of, I would say, risk intelligence platforms being incorporated. That would be something that an integration, higher level of integration should incorporate, if not now, in future at least. And to sum it up, they should provide everything that we've suggested. You know, the logging of the customers, when did the customer onboard, deboard, what was the last log on timestamp. All these things help the regulatory domain, so auditing, compliance at the end of the day. If we are able to provide the customer what they need, making sure that we are

compliant to all the systems, to all the regulations. All these systems, we should make sure that no user information falls out of place. So there's no leak in that way, that the user information doesn't leak. There were some kind of centralized platform controls that we would need to give. We need to make sure that there is all kinds of science, IAM, multifactor, risk intelligence, compliance, and user lifecycle at the end of the day that comes into place.

I: How do you prioritize interoperability and standardized protocols in the context of IAM services?

A: Basically to answer your interoperability question and standardization, there are a few things that we have incorporated. For example, we use all the protocols that are there in the industry, including open ID connect, make sure that we use all these protocols, we make them kind of a seamless integration. We allow the customers to use them. That is what the interoperability is all about, making sure that if the customer comes also with the custom configuration through any of the protocols, we use them. We don't say no, we don't hide ourselves from that, we just adopt it. And we go with the flow, right? How the industry develops. Additionally, I probably said this in the past as well, some of our customers use federations, for example, and on the other hand, they have the option to use APIs. If they might not want to use our own solution, they could, I mean, our own solution would incorporate federations, local plugins, and, you know, incorporating other identity providers. They could also use our API to make sure that they use our robust backend. The customizations are also possible based on their necessities. We just buy them API endpoints so that they can incorporate in their own solution. As I said, for all the industry standards, for example, the OpenID Connect and the SAML and OAuth part, we also make sure that we don't stop the customers to create their own solutions. They have their own IDP configured completely, a solution hosted on their own, you know, on their own environment and stuff. We don't say no to those things. We kind of the neutral people. We say as long as these are industry accepted standards, we are going to use it and they should anyways be compliant to our own standards as well. But I mean, we usually wouldn't say no. We would go with the flow, as I said. And then again, we provide the customers, I would say, I don't know if this is valid, but we provide the customers enhanced testing, right? We don't say that we directly implement in production environment, and you can use it because we are testing them as well. We provide the customer a transparent testing mechanism, making sure that everything that is going into production or into an IP landscape, I would say, is tested, well tested, and maintains the interoperability of the solution at the end of the day.

I: Are there any points from your side that have not yet been addressed but that you would like to add?

A: Yes, there's nothing much. I think I covered almost everything related to it. My points were specifically having to make sure that you're flexible but also making sure that you're future safe in terms of having that observability context in your being more proactive and being reactive. That's the industry, that's the current move to the industry and my only suggestion that I would say to the industry would be to make sure that you are not based on one solution, you use two different solutions at least and make sure that you are future safe in that aspect. So that's the only advice I would have.

I: I sincerely thank you for your willingness and time you have taken to conduct an interview with me. Should you be interested in the results of my bachelor's thesis, I will approach you in September and present them to you.

Appendix 8: Interview Transcript VI

General Data:

Interview-Type	**MS-Teams**
Interview-Number	**6**
Interview Date	**05.08.2024**
Interview-Duration (in Minutes)	

Demographic Data:

Industrial Sector	**Insurance**
Role	**CIAM Product Owner**
Experience in IAM / ITSM (in Years)	**3**

I: Thank you for taking the time to conduct an interview with me as an expert today. Before we start the interview, I would like to briefly introduce myself and give you some information about me. My name is Manuel Yambao and I am in the final stages of my Business Information Technology bachelor's degree at the University for applied Science Ulm and University for applied Science Neu-Ulm.

As part of the interview, I would like to ask you some questions regarding ITSM and IAM services. If you agree to this, please confirm briefly. If you have no questions, I would now like to start the interview. Otherwise, we can clarify any open questions you may have beforehand.

At the beginning of the interview, please tell me about the general tasks you perform in your company.

A: I perform the role as a product owner of the identity and access management tool. Okay so yeah I'm the proxy product owner of a customer identity and access management service for a bigger reinsurance company and my role is to manage the product backlog or the product backlog management of the product and service to ensure that the development continues and we work on developing and providing more services and features around our custom identity and access management service and I'm responsible for product ownership and product development. So, I'm not developing but I'm managing the product backlog and the product development team.

I: What characteristics does an IAM service have that distinguishes it from other IT services?

A: So, there's certain capabilities to enable on and off-boarding to applications or for applications such as automated onboarding or automated provisioning. So, whenever there's like a federation in place with another identity provider or internal other directories, it enables the users to automatically onboard or off-board to internal connected identity and access management system to create necessary roles and permissions via role mapping that we also use. There's also self-service options or capabilities available through certain portals where administrative users can manage user on and off-boarding by themselves through easy user interfaces. And there's also role-based access controls where users get automatically roles or permissions assigned based on groups or roles they are associated with in the system.

I: Can you provide examples of how IAM services respond to frequent application onboarding and off-boarding processes?

A: So well first of all in an identity and access management you have a centralized user management or identity management and access management whereas other IT services might have that more decentralized and user information or identity stored over multiple systems. So, it's easier to manage user

identities and access controls for example. Also, I think the access control level is or capabilities are more granular compared to other IT services or systems so we can provide permissions or user roles via role-based access control for example automatically and just have it more granular and easier to onboard and off-board users automatically for example rather than other IT services where you have to manually interfere or invite users. What else? Yeah you have well I just said that it's centralized so you have a better transparency and overview of the user pool or directory where user identities are stored and have yeah rather than in other services where only a group of or part of the users of the company are stored or have permissions. So yeah, it's more centralized.

I: How does the management of user identities in IAM services differ from that in other IT ser-vices?

A: So well first of all in an identity and access management you have a centralized user management or identity management and access management whereas other IT services might have that more de-centralized and user information or identity stored over multiple systems. So it's easier to manage user identities and access controls for example. Also I think the access control level is or capabilities are more granular compared to other IT services or systems so we can provide permissions or user roles via role-based access control for example automatically and just have it more granular and easier to onboard and off-board users automatically for example rather than other IT services where you have to manually interfere or invite users. What else? Yeah you have well I just said that it's centralized so you have a better transparency and overview of the user pool or directory where user identities are stored and have yeah rather than in other services where only a group of or part of the users of the company are stored or have permissions. So yeah it's more centralized.

I: What strategies do you employ to ensure the scalability of IAM services?

A: Yeah so first of all or most important I think is a cloud-based solution using that as our base architec-ture or infrastructure so to always ensure availability of all resources and ensure that you're scalable because cloud services yeah in themselves offer scalable scalability then having kind of a micro service architecture so you don't have one service or one big infrastructure bank so to say but smaller services in your architecture that are not entangled and detached so you can individually scale those services based on the customer demand or needs in example the self-service capabilities are an own kind of architecture infrastructure set like these portals that we offer based to the base user policies user flow policies that are yeah just in a separate repository than these customer self-service portals so whenever we need to touch one we don't need to touch the other we can scale them independently separate resources for different environments that you can scale individually so yeah.

I: How do you handle variable user loads, and what role does elastic resource allocation play in this context?"

A: so variable user loads first of all we handle first of all by dividing our architecture in multiple environ-ments to really split up the usage of our service for different purposes for testing an example which can deliver a high load of traffic to our services and that can be distinguished or separated from a production environment where real users are signing in so you distinguish or separate those user loads by purpose or by needs and environment and then elastic resource allocation we are using a service that is also offered by another company's IT services which does help us automatically or dynamically allocate re-source traffic or traffic by a different infrastructure regions or infrastructure resources based on the traffic and where it's coming from so where the origin is of that traffic and wherever the load is on the highest to divide or to yeah efficiently reroute the traffic through the most performant or least used resource regions.

I: How do you define 'high effectiveness' in the context of availability management for IAM services?

A: So high effectiveness is uptime first of all so the time that the service is up and running and reliability of the service and well you should all most identity next management service aim for 100% availability there and you could measure those performance metrics by response times latency times error rates for example to you to measure the the reliability of the service or bugs reported.

I: What specific mechanisms do you implement to ensure service continuity for IAM services?

A: So we have a redundancy and failover architecture so we have different or we have multiple replicas of our architecture and resources in different regions or different cloud instances all around the world and we have a failover mechanism implemented that automatically fails over in the scenario of a disaster to one of the other regions or cloud regions, cloud infrastructure resources in the scenario of a disaster so we have a disaster recovery plan also in place that handles these failovers automatic failovers.

I: How is modularity implemented in the service design of IAM services to meet the diverse needs of customers?

A: Well as i said earlier it's important for scalability to have like a micro service architecture so we have a architecture based on different components. Most of these components are basically part of our standard service offering but they don't have to be used they can be used a lot of it available by our self-service portal and more markets out or included to that self-service capability we have also kind of an replica of our capabilities or features via an api connectors or API connectors that can offer them also to customers so it's really flexible and yeah plug and play so to say whatever capability or feature you want to use you can implement that however you want as well via our API connectors which basically replicates or represent the same capabilities we offer or components we offer to our customers using our services as well. we we do have also the capability so we have a standard set of services as well that we offer but we have the capability also to tailor custom tailor diff certain user flow so so the core service that we offer to our customers to have it really customizable in case none of our standard components and services meet the demands of a customer so can also customize highly whatever the customer needs.

I: Can you give an example of how modularity in IAM services affects service provision for internal and external customers?"

A: for example for internal customers the modularity or the modularity of our service offers provides deeper integration with their own systems so for example they can be deeper integrated with the other it services that use our access management. It can be deeper integrated with their own systems and applications for internal customers to use our services and component based or modularity so they might be using our role and access management this also authorization concept we offer or they integrate just our user directory with their application and use their own authorization and user and role management and for external customers an example we offer flexibility by our API to integrate capabilities into their own systems as well so same applies for them yeah cool then

I: To what extent do IAM services require a higher level of integration with other enterprise systems?

A: So usually it requires a high integration with enterprise systems such as HR or enterprise resource planning system or the CRM systems because they need to manage and synchronize the user identities usually. So other enterprise systems need to have access to the user identities in the IAM systems and also the access policies or the roles and permissions of those users to other systems.

I: How do you prioritize interoperability and standardized protocols in the context of IAM services?

A: So it's it's hard you cannot prioritize one over the other so and where interoperability often comes with standardization so we do offer a basic set of our service more highly standardized which makes it easier to include, integrate that to multiple or a wide range of services internally and externally so we're

trying to focus on that to offer standards authentication protocols for example, to everyone like SAML or OpenID Connect to make it interoperable with all other systems.

I: Are there any points from your side that have not yet been addressed but that you would like to add?

A: Nothing to add I guess.

I: I sincerely thank you for your willingness and time you have taken to conduct an interview with me. Should you be interested in the results of my bachelor's thesis, I will approach you in September and present them to you.

Eidesstattliche Erklärung

I herby confirm that the attached bachelor thesis is my own work and that it has not been used for other examination purposes: I have named all the sources and auxiliary material used and I have marked appropriately quotations used verbatim or which I have given the gist of. I tolerate the check using anti-plagiarism software

Place and Date: Signature:

Ulm, 08.09.2024 Manuel Gambao