Bogdanova Anastasiia

Enterprise Resource Planning Authorization Configuration Project. Optimization of SAP license costs

School of Technology and Innovations
Master's thesis
Industrial Systems Analytics

Vaasa 2025

UNIVERSITY OF VAASA
School of Technology
Author: Bogdanova Anastasiia
Title of the Thesis: Enterprise Resource Planning Authorization Configuration Project. Optimization of SAP license costs
Degree: Master of Science in Technology
Programme: Industrial Systems Analytics
Supervisor: Rayko Toshev
Year: 2025 **Pages:** 64

ABSTRACT:
Authorizations in ERP systems are essential for controlling user access to transactions and functions, ensuring that individuals can only perform actions necessary for their roles. This maintains system security and integrity. The topic is particularly relevant for Valmet Automotive Oyj, which is transitioning to the SAP S/4HANA ERP system. The company has decided to manage authorizations internally after the go-live phase, with minimal external support, making the development of a robust authorization concept critical.

The main aim of this thesis is to address research questions: how to handle and maintain SAP authorization errors after the go-live phase, how SAP role maintenance and transport of the role changes is done; what are the ways for minimizing SAP license fees. To achieve these objectives, the study combines a literature review with observations of current processes and data analysis. Additionally, the company's internal authorization concept document was updated with detailed steps and instructions as a deliverable.

The findings include a clear process for managing authorization issues and maintaining SAP roles, as well as the steps, which should be taken to reduce license costs. These measures emphasize adherence to the Principle of Least Privilege, avoiding unnecessary system complexity, and periodically deactivating inactive users. The results are significant for ensuring security and cost efficiency during the ERP transition. The limitations include restrictions of data used for the research and deliverable instruction for the role maintenance process, which is delivered to the company and intended for internal company usage.

KEYWORDS: ERP, TCO of ERP system, SAP, S/4HANA, Authorization Maintenance, SAP Role Maintenance, SAP License cost, Principle of Least Privilege.

Contents

Lists

Tables

Abbreviations

ECC	ERP Central Component
ERP	Enterprise Resource Planning
SAP	Systems Application Product
ECC	ERP Central Component
GUI	Graphical User Interface
SAP S/4HANA	Suite for HANA
User ID, UID	User Identification
RBAC	Role-Based Access Control
GRC	Governance, Risk, and Compliance
CTS	Change and Transport System
IMG	Implementation Guide
ABAP	Advanced Business Application Programming
TR	Transport Request
PoLP	Principle of Least Privilege
GDPR	General Data Protection Regulation
ISO	International Organization for Standardization
NIS2	Network and Information Security Directive
Oyj	Julkinen osakeyhtiö (Public limited company)
vs.	Versus
SOX	Sarbanes-Oxley Act

Disclaimer on Use of AI Tools in Thesis Preparation

I, Bogdanova Anastasiia, hereby acknowledge that I have made use of Artificial Intelligence (AI) tools as part of the thesis writing process. These tools were utilized primarily for the following purposes:

- Proofreading and language refinement;
- Writing assistance in organizing and structuring content;
- Support in drafting the literature review, particularly for theory development and conceptual framing.

While every effort was made to maintain academic integrity, *I understand that the final version of the thesis was flagged with an AI-generated content rate of 21 % and a similarity index of 13%.*

I fully accept responsibility for the implications of this outcome.

Upon review, I was granted a second opportunity by my supervisor to revise and improve the thesis to meet academic standards and originality expectations. I have undertaken this task with sincerity and transparency.

This disclaimer is provided in good faith to affirm my accountability and commitment to academic integrity.

Date: 25.11.2025
Name: Anastasiia Bogdanova
Thesis Title: Enterprise Resource Planning Authorization Configuration Project. Optimization of SAP license costs
Institution: University of Vaasa, Finland

1 Introduction

Authorizations in ERP systems are crucial for controlling user access to various transactions and functions within the system. Authorizations help to ensure that users can only perform actions and access data that is necessary for their daily work-related activities, thus maintaining the security and integrity of the system.

The work was conducted for the company Valmet Automotive Oyj, which is on the way of transitioning to new S/4HANA ERP system on the moment of writing this thesis. Thesis work covers process design of handling and maintaining SAP authorization errors for the post go-live period. On the moment of writing, the plan is to continue maintenance of authorizations internally, with the minimal external support.

During the project there has been created new Authorization Concept. The changes to the existing and creation of new SAP roles should be made in accordance with the New Authorization Concept. As a deliverable this thesis work will provide an overview of the Authorization Concept, the instructions for SAP role maintenance and transports of authorizations will be created for the company but included in the thesis as a superficial description.

The company wants to pay minimum SAP license costs, therefore the ways of minimizing the license costs are planned to be found as one more outcome of the research.

One of the real-life examples of indirect access of the SAP software, which brought up the ambiguity for the indirect license usage for further and existing customers was the case with customer company of SAP, which was considered in the court in 2017. In overall SAP sued client company in the United Kingdom Hight Court for indirect usage of the SAP software. Defender initially accessed SAP software directly for managing customer's orders but with the time moved to the cloud product, provided by the third-party, and as a result of this transmission it became possible to manage customer orders in the third-party system and supposedly access SAP software indirectly, which was not

compliant with the SAP licenses. As a result of the dispute SAP has been awarded up to £54 million in damages. (Martin, Bajowala, Borich, Powell, 2017). Assuming that nowadays there are quite many solutions, which can be indirectly connected to the SAP software, this topic is quite highly important towards the license costs and company's reputation.

1.1 Background

The background chapter examines the underlying factors contributing to inefficiencies in SAP license cost management. It explores how organizational practices, such as unstructured role assignment and limited visibility into actual system usage, lead to the allocation of higher-cost licenses to users whose functional requirements do not justify such access. These behaviors are further compounded by the complexity of SAP's licensing framework and the absence of systematic governance mechanisms. To address these challenges the chapter describes a set of preventive processes and controls. These include the implementation of role-based access control (RBAC), regular audits of user activity, and periodic internal reviews of license classifications. Additionally, the chapter emphasizes the importance of aligning license management with principles such as the Principle of Least Privilege (PoLP), which ensures that users are granted only the minimum access necessary to perform their daily work-related tasks. All together these strategies aim to avoid extra expenses and make operations more cost-effective, mitigate compliance risks and support smooth operation of the ERP system.

Transitioning to SAP S/4HANA represents a significant shift not only in technology but also in business process architecture. One of the most crucial aspects of this transformation is the development of a comprehensive authorization concept, which governs user access and ensures compliance, security, and operational efficiency.

The next three paragraphs focus on SAP user license fees, key cost drivers and their broader strategic impact. SAP user license fees are a critical component of ERP cost

management, yet they remain highly variable and contract dependent. Academic and industry sources consistently highlight that SAP licensing is influenced by multiple factors, including deployment model (on-premise vs. cloud), license type (named user, engine-based, or consumption-based), and organizational size and structure.

According to ERP Research, SAP S/4HANA implementations typically range from $250,000 to several million dollars annually, depending on the number of users, modules, and infrastructure requirements. Reveal Compliance further explains that SAP offers both perpetual and subscription-based licenses, with named user licenses priced according to user roles and access levels. Misclassification of user roles—such as assigning professional licenses to self-service users—can lead to significant overpayment, a concern echoed in SAP Community discussions.

Effective license management requires aligning of user's access with actual usage patterns and business requirements. This includes carrying out regular audits, using tools such as USMM and SLAW, and applying role-based access controls to make sure licenses are used efficiently and correctly.

1.1.1 Security and Compliance

SAP S/4HANA introduces a simplified data model and new user interfaces (e.g., SAP Fiori), which require a re-evaluation of existing roles and authorizations. Without a well-defined authorization concept, organizations risk exposing sensitive data or violating compliance requirements such as GDPR or SOX.

Kulkarni (2019) emphasizes that authorization design must be aligned with the technical architecture and organizational change management strategies during S/4HANA implementation. He notes that inadequate planning in this area can lead to project delays and increased audit risks.

1.1.2 Role redesign and Optimization

The transition from SAP ECC to S/4HANA necessitates a comprehensive redesign of user roles, driven by changes in transaction codes and the adoption of SAP Fiori applications. This redesign extends beyond technical adjustments—it must align with the evolving organizational structure and user responsibilities. Haddara (2012) highlights that ERP adoption costs are significantly influenced by the complexity of role configuration and access control, especially when adapting to new system architectures. Furthermore, deployment choices—whether on-premises, cloud, or hybrid—introduce varying cost and management implications for role standardization. A well-defined authorization concept not only mitigates these costs but also ensures consistency and efficiency across the chosen deployment model. (Haddara, 2012).

1.1.3 Project efficiency and Risk Mitigation

A well-defined authorization strategy plays a pivotal role in facilitating the testing, training, and deployment phases of an ERP implementation. It enables early detection of access-related issues, thereby minimizing disruptions and reducing the likelihood of last-minute modifications that could compromise project timelines. Haddara (2012) identifies access control and role configuration as significant cost factors in ERP adoption, emphasizing that insufficient planning in these areas can lead to increased implementation complexity and resource expenditure. Integrating authorization design into the broader project management framework—as advocated by Kulkarni—supports proactive governance and enhances the predictability of implementation outcomes. (Haddara, 2012).

1.1.4 Embedded Analytics and Real-Time access

The advanced embedded analytics capabilities of SAP S/4HANA necessitate stringent control over data access to ensure that users interact only with information pertinent to their roles. While Pattanayak (2017) emphasizes the technical need for fine-grained

authorization models to support real-time analytics, Haddara et al. (2022) highlight a broader organizational challenge: in cloud-based ERP environments, particularly within SMEs, managing access control becomes increasingly complex due to multi-tenant architectures and dynamic user roles. These challenge show why having a strong authorization concept is important, especially in areas of healthcare and finance, where legal requirements demand to carefully separate the data and be able to track users' access. (Pattanayak, 2017) (Haddara et al., 2022).

1.1.5 Principle of Least Privilege in SAP Authorization Management

The Principle of Least Privilege (PoLP) is a foundational concept in SAP authorization design, aimed at minimizing security risks by granting users only the access necessary to perform their job functions. This principle is especially critical in ERP environments, where overprovisioned access can lead to data breaches, fraud, and regulatory violations (National Institute of Standards and Technology [NIST], 2020).

GRC Advisory reports that in a study of 225 organizations, 85% of assigned SAP authorizations were unused in the last 90 days, and one-third of users had access to systems they never logged into. Such findings underscore the prevalence of excessive access and the need for stricter role governance. The SAP Help Portal reinforces this by detailing how PoLP is enforced through service bindings and access tokens, ensuring that applications and users are restricted to specific namespaces and operations (National Institute of Standards and Technology [NIST], 2020).

Academic research by Abbas (2024) further supports PoLP as a key strategy for reducing attack surfaces and mitigating insider threats. When combined with Segregation of Duties (SoD), PoLP enhances organizational security and supports compliance with frameworks like GDPR and SOX (National Institute of Standards and Technology [NIST], 2020).

Implementing PoLP in SAP involves regular role reviews, usage audits, and the adoption of just-in-time access models to ensure that privileges are granted only when necessary and revoked promptly thereafter (National Institute of Standards and Technology [NIST], 2020).

1.1.6 Software License selection and proliferation faced by legal

The use of standardized, pre-approved open-source licenses—such as those endorsed by the Open Source Initiative (OSI)—is widely encouraged due to their clarity and reduced legal overhead. These licenses function as templates, streamlining legal review and minimizing negotiation efforts. However, when existing licenses do not meet specific project needs, some developers opt to create custom licenses. This practice, known as license proliferation, is generally discouraged as it increases compliance complexity and introduces compatibility challenges. Experts and open-source organizations advocate for minimizing the creation of new licenses to preserve interoperability and reduce the burden of legal vetting. Although license proliferation was a notable issue in the mid-2000s, it has declined in recent years due to growing awareness of the benefits of using well-understood, standardized licenses (Wintersgill et al., 2024).

The study identifies several critical challenges and practices related to OSS licensing and compliance. First, while obtaining license exceptions is a recognized practice, it is often hindered by the inability to contact original project authors, complicating the negotiation process. License changes, including proprietary relicensing and multi-licensing, are driven by diverse motivations but can disrupt dependent projects and lead to fragmentation through forking (Wintersgill et al., 2024).

Non-compliance is prevalent within the OSS ecosystem, largely due to the complexity of maintaining license adherence. Such violations affect not only the infringing parties but also users and the broader community, potentially delaying development and release cycles. Enforcement mechanisms are predominantly community-driven, with limited

formal legal action; informal methods such as public accountability are more commonly employed (Wintersgill et al., 2024).

Effective compliance is best achieved when integrated throughout the development lifecycle rather than addressed retrospectively. Although compliance requires collaboration among developers, legal professionals, and organizational stakeholders, it is often perceived as the developer's responsibility. Larger organizations may establish Open Source Program Offices (OSPOs) to support and coordinate compliance efforts (Wintersgill et al., 2024).

Tracking software provenance remains a significant challenge, yet it is essential for ensuring license conformity. Risk management practices vary across organizations and are influenced by jurisdictional and cultural factors. Moreover, developers frequently lack comprehensive understanding of licensing obligations, underscoring the need for targeted training and accessible legal resources (Wintersgill et al., 2024).

Organizations increasingly rely on automated tools to identify software components and associated licenses. However, these tools often lack interpretive capabilities and generate false positives, limiting their practical utility. The growing complexity of software systems, characterized by numerous dependencies, further complicates legal compliance efforts (Wintersgill et al., 2024).

Finally, OSS licenses present interpretive difficulties due to their static nature and the evolving technological landscape. The absence of authoritative legal guidance compels lawyers to rely on community norms and informal documentation. Communication between legal and technical teams is often strained by differing perspectives on intellectual property and organizational expectations, highlighting the need for improved interdisciplinary collaboration (Wintersgill et al., 2024).

1.2 Valmet Automotive Oyj

Valmet Automotive has been founded in 1968. It is best known as vehicle partner Manufacturer on behalf of the renowned OEMs. Valmet Automotive is also known as a partner of Mercedes-Benz, Saab and Porsche. More than 1.8 million vehicles have been built on the factory in Uusikaupunki, Finland. Another Business Line of Valmet Automotive produces roof and kinematic systems, such as convertible roof systems, active spoilers and loading flaps.

In 2018 the company spread its area of expertise and began producing electric batteries by establishing new Electric Vehicles business line. In 2024 its Electric Vehicle business line became independent entity and transitioned to be a new company named IONCOR. Rebranding took effect in October 2024.

1.3 Research objectives

First research objective is to design authorization analysis and maintenance process by performing literature review, observing current process for the ECC system and maintenance of authorizations during the project.

Second objective is to identify the ways and activities for minimizing SAP license costs. This objective will be achieved by literature review and analysis of unused active user accounts in the current productive SAP ERP system. For this analysis there is going to be used two time periods and identify most appropriate timeframes for deactivation unused user accounts. It means that if during defined period of time the user have not logged in to the SAP ERP system, his user account can be deactivated, and the license data can be removed. In terms of minimizing the costs the TCO concept and Software Service Models will be described.

Third research objective is provision of instructions for authorization maintenance process, which can be used as a reference for the Role Design Document. This document will be based on the theoretical part of this thesis. The instruction will be delivered to the customer company directly and not published as a part of the thesis, but the overview of the process will be described.

1.4 Research questions

The research is directed by several research questions, which are outlined in this subchapter. First research question is: How SAP role maintenance is done? Second question is: What is the process of transporting the change made for the SAP role to the productive system? Third question is: How to minimize costs for the SAP licenses and what should be done to keep them on the minimum level after go-live?

1.4.1 Research question 1

To give an answer for the first research question: “How SAP role maintenance is done?” the literature review has been made along with the analysis of role maintenance processes, which are established in the currently used SAP ERP Productive system. The way changes are done during the project of implementing SAP S/4HANA system has been observed. The theory part of this thesis work covers basic and major principles, which should be taken into account, when maintaining SAP roles, including part of critical authorization objects and importance of naming convention definition.

1.4.2 Research question 2

Second research question of this thesis work is: “What is the process of transporting the change made for the SAP role to the productive system? To answer this question the literature review has been done and processes used for the SAP role maintenance in the

currently used Productive and new S/4HANA systems are observed and optimum solution defined.

1.4.3 Research question 3

Third research question is: How to minimize costs for the SAP licenses and what should be done to keep them on the minimum level after the go-live? To answer these questions, the data from the currently used ERP SAP system has been collected and analyzed and calculations were made along with literature review. In the theory part cloud software solutions are introduced and topic of cost difference is opened.

1.5 Structure of the study

Initiation of the study is done in the Chapter 1, which provides the overview of the study, company description, research objectives and research questions.

Chapter 2 consists of the Literature review, which includes general overview of the ERP SAP S/4HANA system and Cloud Computing Software Models description, opens topic of authorization from the critical authorization objects and system point of view, highlights the importance of the naming convention, outlines Principle of Least Privilege, gives overview of the Change and Transport System, SAP licensing concept and Total Cost of Ownership of the EPR system.

Chapter 3 illustrates research methodology, description of the selection criteria for the data utilized for the analysis as well as observations, based on the results of the data analysis. Details for the TCO calculation are included in the chapter.

Chapter 4 consists of research findings about the process of SAP role maintenance and transport throughout the system landscape, where process overview is described. Next

subchapter summarizes how to keep license cost at the low level. Validity and reliability of the study and managerial implications can be found in the same chapter.

Chapter 5 provides a comprehensive summary of the study's findings, followed by conclusions drawn from the analyses.

1.6 Limitations

First research question will be covered in a separate internal document, which will provide the instructions for authorization maintenance process and transport of the changes, related to authorization. It will not be included in this thesis work, but overview will be added.

For the research question related to minimizing SAP license costs, initial plan was to export the numerical data for the users, who have not logged in to VHP and make comparison to the Fiori instance: exclude users who use Fiori from the data set, as it is necessary to have active user account in VHP in order to use SAP Fiori system. But user data comparison between GUI and Fiori interfaces has been placed under the limitation, because of several uncertainties. In Fiori instance users had different last log on date - it was not clear which time period can be considered to exclude the users, who do not use Fiori anymore. Also, some of the users who has not been using SAP user account in VHP (GUI), had recently created user account in Fiori. The user account was created 1-3 months ago from the time the research was made. It brought another uncertainty if this type of users should be considered, and if yes, what should be the period of remaining the active misused user account in the system. Therefore, additional limitation has been taken into account on the stage of data cleaning and usage of Fiori Productive system has not been considered for the limitation of the research data.

The period for which the research data has been exported from the system is limited to 10 months. This limitation can be explained by the fact that customer company conducts regular user audits and deactivates unused user account in the system.

2 Literature review

2.1 Implementation of SAP S/4HANA ERP system

SAP S/4HANA is an enterprise resource planning software system, whose predecessors are SAP R/3 and SAP ERP. The SAP HANA platform became available since 2010. The purpose of the platform is to cover daily end-to-end processes of a company, as for example procure-to pay, order-to-cash, plan to product and request-to service (SAP LeanIX, 2024).

There are several approached to software system implementation. By following Greenfield implementation approach the enterprise has an opportunity for reengineering company's SAP processes and workflows. No customization from the SAP ECC can be utilized, if this approach is selected. The implementation is started from the clean state. The advantage of this approach is possibility to simplify the workflows comparing to the legacy system, which has been used for a long time period. From another point of view the Greenfield approach is the riskiest among all other implementation approaches, because all critical customizations have to be carefully redeveloped, what is quite time consuming. Another scenario is when the enterprise starts transition to SAP S4/HANA with the blank state in some selective areas to reduce the complexity of the business processes, simplify customized code and integrations - "Selective Greenfield" implementation approach is used (SAP LeanIX, 2024).

While Greenfield approach implies redesign of the workflows, business processes and customized codes, Brownfield approach stands for the upgrade. Brownfield approach allows migration of the existing and proven SAP workflows and customization to the new version of SAP S4/HANA. The disadvantage of this approach is that due to migration the innovations might be neglected. But mostly it depends on the degree of replication of existing workflows and systems. Brownfield implementation approach allows customers to use their own current solutions, while transferring to the new SAP S4/HANA system during minimum timeframe (SAP LeanIX, 2024).

Hybrid approach combines Greenfield and Brownfield implementation methods. This approach is recommended to the large companies. The company has a chance to decide what should be resigned and what can be kept in the new system. The challenge of the approach is necessity of usage of the third-party tool for implementing the job and separate pieces of both approaches, which intend to be part of the migration plan (SAP LeanIX, 2024).

2.2 Cloud Computing Software Models

M. Kavis is bringing an example of the Instagram, photo and video sharing social networking application, which was launched in 2010 and acquired quick and huge growth in users in a very short period of time. Due to selecting cloud platform and transfer responsibility for the hardware, data centers, network maintenance, software engineers had ability to focus on the application architecture and user experience, what turned to be a great success in the end. The “Instagram case” was the example of cloud platform selection for the new startup, for which the cloud implementation was the initial and did not require as much effort as for the companies with the existing data centers, for which the transition can be challenging. M. Kavis provides an example for Netflix – industry leading streaming service company – for which high traffic volume became the reason of transitioning to the cloud. Company is convinced that usage of cloud computing brings them competitive advantage on the market and allows to control the costs and lower risks of the downtime. Moreover, high demand on the cloud computing from the enterprises forms competitive environment for the cloud service providers, which helps drive innovations and lower the prices at the same time. (Kavis, 2014).

Riot Games, the developer of the popular video game League of Legends, transitioned its infrastructure to Amazon Web Services (AWS) to enhance scalability, reliability, and performance in supporting its global player base. By utilizing AWS’s cloud computing capabilities, Riot Games was able to efficiently manage the fluctuating traffic demands caused by millions of concurrent users. Migration to AWS ensured smoother gaming

worldwide together with improving response time. Additionally with AWS game updates and patches could be deployed faster, making operations more flexible. The integration of AWS's cloud solutions not only optimized infrastructure costs but also enabled Riot Games to scale its operations more effectively, ultimately enhancing the overall user experience (Amazon Web Services, 2025).

As per Velkoski et al., companies would see considerable reduction in their CAPEX and OPEX, as a result of migration of their business information systems to cloud platforms. In addition, as there is broad number of services available in the cloud, with cloud transitioning the company could get new opportunities for business growth. (Velkoski et al., 2014).

Armbrust et al. (2010) discuss the transformative impact of cloud computing, emphasizing that businesses can utilize the cloud's ability to adapt to increased demands and flexibility to quickly scale operations and enter new markets. The authors argue that the cloud enables organizations to access computing resources on-demand, which not only reduces the financial barriers associated with traditional IT infrastructure but also creates opportunities for business expansion. By adopting cloud solutions, companies can respond more efficiently to fluctuations in demand, innovate more rapidly, and position themselves for growth in dynamic market environments.

The principal models of cloud computing offered by the cloud providers are SaaS – Software as a Service, PaaS – Platform as a Service and IaaS – Infrastructure as a service. Figure 1 displays IT service responsibilities for each model for the customer and cloud service provider: customer's responsibility is colored in red, green colored is the cloud service provider responsibility. The company owns full responsibility for the IT management, in case if "On Premise" model is selected. Selection of IaaS transfers part of the responsibility to the cloud server provider: management of the hypervisor and virtual machines (virtualization), hardware infrastructure (servers, storage and data centers) and global connections between the data centers (networking), what reduces

requirement for network and equipment administration from the customer's side. Cloud service provider is also responsible for basic security in this model; there is an option to include backup disaster recovery in their responsibility when subscribing for this service. PaaS customers transfer the responsibility for the system software to the cloud providers. SaaS subscribers are exempted of business information system administration and maintenance – whole responsibility is transmitted to the cloud service provider (Velkoski et al., 2014).

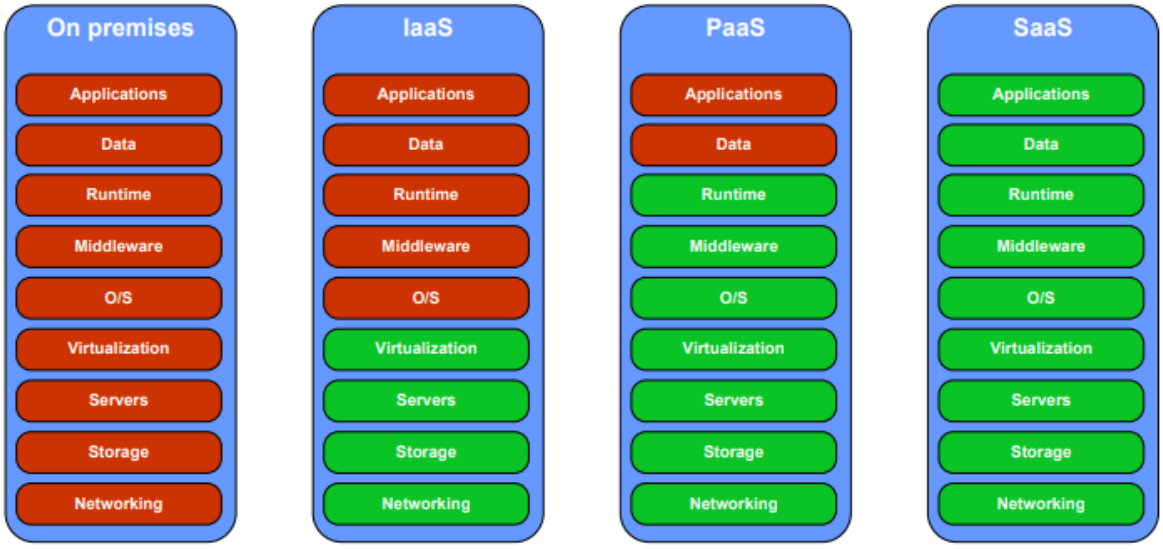


Figure 1. Comparison between the cloud service layers (IaaS, PaaS and SaaS) and on-premise computing (Velkoski et al., 2014, p. 803).

Depending on the cloud solution type and provider's business model various licensing models are available. Subscription-based licensing includes system support and updates, it requires user to pay for selected time-period. Positive side is the flexibility – user is able to make changes for the provided services, but the minus is that the license is limited by the subscription period. User-Based Licenses are stick to the single users, easily manageable but can be expensive, in case of a large amount of users. Device-based licensing, when the license is assigned to the device, is suitable for common usage of several people from the same device, which can be expressed as a minus – the number of devices is restricted to one. Usage-Based Licensing is based on the number of consumed resources, which is optimal for the variable load, but amount of the expenses can be

unpredictable. Transaction-based licensing implies payment for every transaction or operation: which can be profitable, when not much usage is needed but incur high costs in case of the workload increase. (Velkoski et al., 2014).

The pricing of software licenses can also be highly dependent on vendor relationships and negotiation power. Larger organizations often have the ability to negotiate more favorable terms, while smaller companies may face more restrictive licensing costs. This phenomenon is especially notable in enterprise software solutions. Many software vendors, such as Microsoft, Oracle, and SAP, use a complex pricing structure that varies by business size, industry, and regional market. As noted by Krause et al. (2021), these variations can create significant cost dependencies based on the vendor's market positioning and the license type (e.g., perpetual, subscription, or floating licenses).

Velkoski et al. (2014) highlights another factor which influence on the software license costs is the deployment model. The software can be deployed in Public Cloud, Private Cloud, Hybrid Cloud or Multi-Cloud. In Public Cloud the license is provided by the software provider, no necessity to purchase licenses separately. For Private-Cloud usage licenses should be purchased separately. For Hybrid Cloud deployment model there is a mix of local and cloud licenses available. Multi-Cloud deployment model implies payment of cloud independent license fee or separate agreements with multiple software providers.

2.2.1 Deployment models

In Architecting the Cloud, Michael J. Kavis discusses several cloud deployment models that organizations can adopt based on their specific requirements, including public, private, hybrid, and community clouds. Each model offers different benefits and trade-offs in terms of control, security, scalability, and cost. (Kavis, 2014).

A public cloud is one where the cloud infrastructure is owned and operated by a third-

party cloud service provider and is available to the general public. Providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud offer public cloud services that customers can access on a pay-as-you-go basis. (Kavis, 2014). This model allows organizations to use and access infrastructure and software without the need for significant upfront investment in hardware or software. The public cloud offers a high degree of scalability and flexibility, making it suitable for businesses of all sizes that need to quickly scale their operations. It also lowers ownership costs by removing the need for on-site maintenance, physical hardware, and IT personnel. The public cloud can help optimize expenses, since companies only pay for what they actually use, what is more cost-efficient compared to running infrastructure on-premises. (Marinescu, 2017).

Public cloud characteristics include shared resources, where multiple organizations use the same physical infrastructure. This setup allows cloud providers to scale resources dynamically based on demand, providing a cost-effective solution since organizations only pay for what they use. Public clouds are highly accessible, as services are available over the internet, making them easy to access from anywhere. These features make public clouds ideal for organizations that do not deal with sensitive data or strict compliance needs, or for applications requiring rapid scaling without the need for extensive customization (Kavis, 2014). According to Marinescu (2017), one of the most significant cost-related advantages of the public cloud is its ability to provide businesses with the flexibility to adjust resource usage on demand. The pay-per-use model allows businesses to scale computing resources up or down based on real-time needs, meaning that businesses can avoid unnecessary expenses associated with maintaining idle infrastructure. By eliminating the need for large capital expenditures and reducing operational overhead (such as IT maintenance), public cloud services provide businesses with a highly cost-effective IT solution, especially for businesses with fluctuating or unpredictable resource demands (Marinescu, 2017).

Another deployment model is a private cloud. A private cloud is a cloud environment dedicated solely to one organization. It can be hosted on-premises or by a third-party

provider, but it is not shared with other organizations. This model offers more control over the cloud environment and security (Kavis, 2014). The private cloud deployment model offers several cost-related advantages, especially for large organizations. While it typically requires higher initial investments in dedicated hardware and infrastructure, it can lead to significant long-term cost savings by allowing businesses to leverage existing resources more efficiently. Private clouds enable predictable costs, as organizations can avoid the variable charges of public cloud models and instead plan for stable, fixed expenses. Moreover, the model provides businesses with greater control over security and compliance, reducing the need for external service providers and making it easier to meet specific regulatory requirements. Over time, private clouds can also optimize resource usage, enhancing the efficiency of IT systems and leading to lower operational costs compared to traditional on-premises setups (Armbrust et al., 2010).

Private clouds, on the other hand, offer exclusive ownership, where the infrastructure is dedicated to a single organization. This provides enhanced security and control since the environment is not shared, allowing for greater customization and better security measures. However, private clouds generally involve higher costs due to the larger upfront investment in hardware, software, and ongoing maintenance. Private clouds are best suited for organizations with stringent security, compliance, or performance requirements, or those that need to keep sensitive data within their own environment (Kavis, 2014).

Third deployment model is a hybrid cloud. A hybrid cloud is a combination of both public and private clouds, allowing for the sharing of data and applications between the two. This model enables organizations to take advantage of the scalability of the public cloud while retaining critical workloads in the private cloud. Hybrid clouds combine the flexibility of both private and public clouds, allowing workloads to move between them based on demand, cost, or security considerations. This model optimizes resources by keeping sensitive data and critical applications on the private cloud while using the cost-effective public cloud for non-sensitive applications. However, managing hybrid clouds

can be complex, requiring sophisticated orchestration tools. Hybrid clouds are ideal for organizations that need to balance workloads across both cloud types, keeping mission-critical data private while benefiting from the elasticity of the public cloud for less sensitive operations (Kavis, 2014). The hybrid cloud deployment model offers several advantages, including flexibility and scalability, as it allows organizations to leverage both public and private cloud resources based on their needs. This can result in cost efficiency, especially for businesses with fluctuating workloads, by enabling the use of public cloud for less sensitive tasks while maintaining control over critical operations in the private cloud. However, there are notable challenges, such as the complexity of integration between public and private cloud infrastructures, which can lead to interoperability issues. Additionally, while hybrid clouds provide more control over data, they still raise concerns about security and compliance, especially when managing data across multiple environments. The model also requires increased management resources and expertise, leading to higher operational overhead (Rimal et al., 2011).

A community cloud is a collaborative effort where infrastructure is shared by several organizations with common interests, such as regulatory compliance or industry-specific requirements. This type of cloud is less common but useful for organizations that need to share resources in a secure, cost-effective way (Kavis, 2014). The community cloud model allows organizations to meet specific security and compliance requirements while optimizing resource usage. It provides cost savings and benefits of collaboration. However, challenges include the complexity of governance and coordination between organizations, and the security risks associated with shared infrastructure. Effective management of these aspects is critical for ensuring the model's success (Sotomayor et al., 2009).

Community clouds involve shared environments where infrastructure is used by several organizations, but access is restricted to members of the community. The costs of the cloud infrastructure are split among these organizations, making it more affordable than a private cloud. Community clouds are typically designed to meet the specific needs of the community, such as regulatory requirements or industry-specific standards. This

model is ideal for industries like healthcare, finance, or government, where organizations share common compliance or regulatory needs but do not want to fully manage their own private cloud (Kavis, 2014). The community cloud model offers significant cost benefits, primarily through cost sharing among organizations with common needs. By sharing infrastructure, organizations reduce their capital and maintenance costs, achieving economies of scale. This model also improves resource utilization, leading to lower operational costs compared to traditional on-premises setups. Additionally, it can reduce IT overhead by outsourcing management tasks like hardware maintenance (Marinescu, 2017).

Michael J. Kavis emphasizes that selecting the appropriate cloud deployment model requires careful consideration of various factors, including security and compliance, cost efficiency, flexibility, scalability, and management control. Organizations with strict regulatory requirements may prefer private or community clouds for enhanced security, while public clouds offer a more affordable solution for those seeking to avoid significant capital expenditures. Hybrid clouds provide scalability, making them ideal for organizations with fluctuating resource demands, and private or community clouds are better suited for businesses that need greater control over their cloud infrastructure. Ultimately, Kavis underscores that the choice of deployment model must align with both the organization’s immediate needs and long-term objectives, considering its business goals, budget, security, and management preferences (Kavis, 2014).

The key takeaway from Kavis’ book is that organizations must consider both their immediate and long-term needs when selecting a deployment model. The deployment model chosen should align with the organization’s business objectives, budget constraints, security requirements, and the level of management they are willing to invest in (Kavis, 2014). When selecting a software deployment model, organizations must consider several factors, including cost, scalability, security, and control. The model should align with the organization's budget and allow for scalable growth without significant upfront investment, especially for businesses with fluctuating needs. For example, the public cloud

is often more cost-effective and scalable, while private clouds offer greater control and security, which may be important for industries with strict regulatory requirements. Another key factor is the organization's technical expertise, as some models require specialized skills for management and maintenance. Vendor lock-in is also a consideration, as reliance on a single provider may limit flexibility. Ultimately, choosing the right deployment model depends on balancing these factors to meet both business objectives and technical needs (Harrison & Lainhart, 2015).

2.2.2 Software as a Service (SaaS)

SaaS is the abbreviation for "Software as a Service". This application model is developed based on the agreements with the SaaS provider, which covers such aspects as service level agreement, network protocols, security, etc. (Liao, 2009). SaaS assumes delivery of the entire application to the customer including everything related to the service delivery as infrastructure, application logic, deployments etc. (Kavis, 2014) Deployment of such application is done on the internet servers and the customers can get access to the required system modules by leasing them from vendor, in accordance with the user amount, for whom the system is needed, or based on the subscription type. (Liao, 2009). Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), accounting and payroll are the most frequent applications, for which customers decide to take in use SaaS (Kavis, 2014).

SaaS selection exempts client companies from taking such many resources and time on their non-core functions, comparing to on-premise model selection, freeing up the time for concentrating on their core tasks. Consumers have access to the systems via the browser and internet connection, for which they are charged a subscription fee. (Kavis, 2014). The Software as a Service (SaaS) deployment model is highly cost-effective for businesses, as it eliminates the need for substantial upfront investments in hardware and infrastructure. Organizations only pay for what they use, with subscription-based pricing that reduces capital expenditure and allows for predictable operational costs.

Additionally, SaaS providers handle software maintenance, updates, and security, which minimizes the need for in-house IT staff and reduces ongoing maintenance costs. This makes SaaS particularly appealing for small to medium-sized businesses with limited IT resources (Marinescu, 2017).

2.2.3 Platform as a Service (PaaS)

PaaS is another level in stack, which is on the top of IaaS. PaaS offers facilitate deployments, without spending costs on buying the hardware, which is provided by the cloud service provider and can be accessed via the internet. The customer controls deployed applications and able to control the application environment setting, while cloud provider is responsible for cloud infrastructure, servers, networks, operation systems and storage. It provides a cost-effective way to quickly develop and deploy new applications, reduces the amount of coding for the developer and fees for the time for the software customizing by exempting him from maintaining the software. (Kavis, 2014). PaaS deployment model offers significant cost advantages by providing a managed environment for developing, testing, and deploying applications. PaaS eliminates the need for businesses to invest in and maintain the underlying infrastructure, such as servers and networking hardware, which reduces both capital expenses and operational costs. Furthermore, it allows businesses to scale applications easily without worrying about capacity planning or hardware management. By using PaaS, organizations can focus on development and innovation, while the provider manages software updates, security, and infrastructure, lowering overall IT maintenance costs (Zhang, Cheng, & Boutaba, 2010).

2.2.4 Infrastructure as a service (IaaS)

IaaS is one of the cloud service models, which is characterized by the standard organization for cloud security - Cloud Security Alliance (CSA) as the model which provides as a service computer infrastructure, networking and raw storage. Consumers are exempted

from buying physical data centers and infrastructure but instead purchase required resources as an outsourced service. (Kavis, 2014).

On the figure 2 there is reflected statistics for organizations' choice of the IaaS providers in years 2021-2024. 2961 respondents participated in the online survey for the IT management professionals published by Lionel Sujay Vailshery in December 2024. More than half of the worldwide respondents indicated that their company was planning or already used Azure. There was a significant deviation (25% in 2024 instead of 38% in 2023) when comparing the respondents voted for IBM last years. (Statista, 2024).

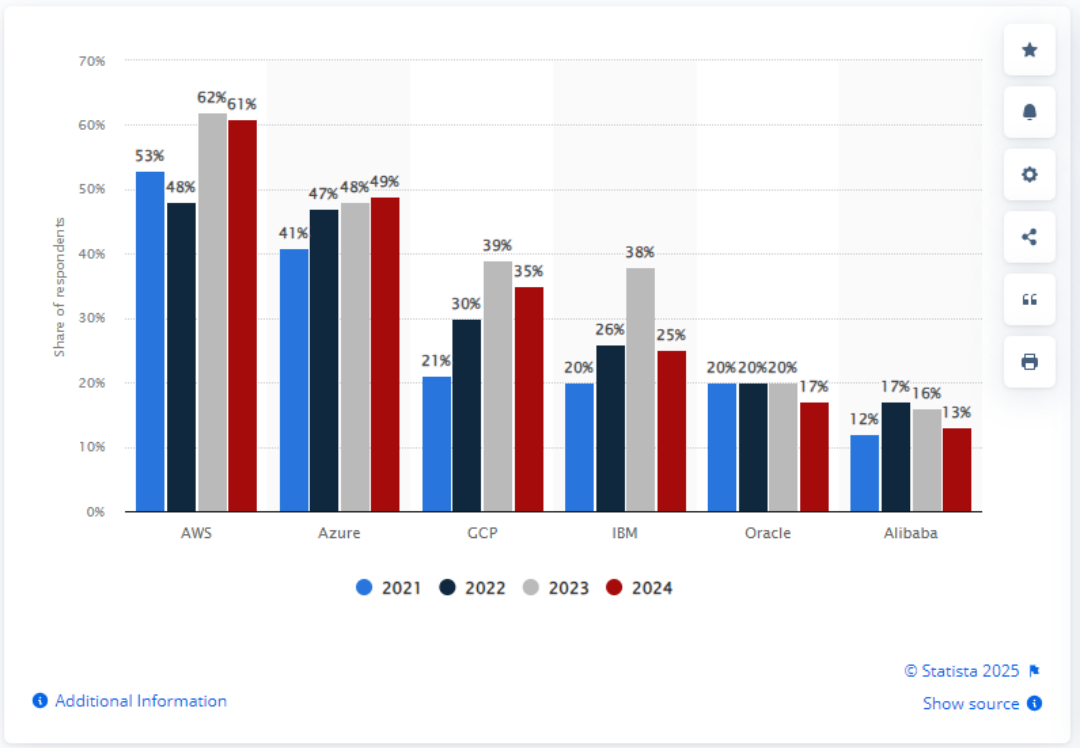


Figure 2. Organizations choice of cloud IaaS providers worldwide from 2021 to 2024. (Statista, 2024).

2.3 Authorizations in SAP ERP system

Authentication and authorization are crucial security procedures employed by system administrators to protect systems and data. These two terms frequently cause misunderstandings. Authentication is the process for verifying user identity, in order to grant

access to the system. Standard authentication tools, available for all SAP NetWeaver systems, include user ID and password. The user can still authenticate himself in the system even without authorizations to specific functions. Authorization, on the other hand, determines the level of access rights for the user. Access rights are permissions granted to users or systems that define the extent of access to resources, such as data, available in the system. These rights are usually assigned based on the business roles and job responsibilities. (Banzer, 2022).

Role Based Access Control (RBAC) within SAP is an approach that manages authorizations through roles, which are essentially defined sets of privileges within the system. These privileges are tied to authorization objects that control access to various transactions and functions, ensuring that users only have the permissions necessary to perform their jobs. (Linkies & Off, 2006).

In the context of security within SAP, authorization objects are key elements that represent the specific fields or data which users can access. Every transaction in SAP requires certain authorization objects to be allocated to the user, which effectively controls what the user can do within the specific transaction. (Hirao J. & Wun-Young, L., 2009; Lamotte-Schubert, M., & Weidenbach, 2009).

By using RBAC, SAP systems allow implementation of the Principle of Least Privilege, making sure that users are not granted more access than what is required for their role. This concept is crucially employed in adhering to security best practices and is central to complying with data protection regulations such as the General Data Protection Regulation, in short GDPR, as indicated in various security renewal projects (Mast, 2018).
In conjunction with the roles and authorization objects, SAP systems can also embody the 'four eyes principle', which enhances security, especially for critical operations and documents that require at least two persons to review and approve actions, thus minimizing the risk of error or fraud (Osaci et al., 2018).

A sophisticated RBAC system in SAP enables organizations to manage the life cycle of user access effectively, as it provides a structured and granular approach to controlling what users can see and do within the system. Roles become containers for authorization objects, which can then be managed more coherently (Buecker et al., 2012).

This model allows to prevent segregation of duties conflicts and potential fraud by ensuring that critical tasks are not concentrated with a single user. SAP GRC Control, for instance, is a tool that can be used for analyzing critical authorization objects and roles, it helps organizations to monitor and manage the risks associated with user privileges (González, 2016).

In essence, RBAC in SAP is a model that allows for streamlined management of user permissions, which is fundamental in maintaining a secure and compliant IT environment (González, 2016).

2.4 Naming convention

It is important to follow naming convention for SAP roles, catalogs, spaces, pages and groups for ensuring transparency and clarity in role management procedures. Usage of naming convention simplifies identification of the required role and the role assignment to the end user and minimizes the risk of errors in assigning inappropriate or unnecessary authorizations to the users. Therefore, well-defined naming convention supports administrators in their daily activities (Chuprunov, 2013). A well-defined naming convention for SAP roles and catalogs is critical for maintaining clarity, consistency, and security in the management of user authorizations. According to Gupta et al. (2016), a structured naming system facilitates the efficient administration of roles by making it easier to categorize and identify specific roles based on their function, scope, or organizational unit. This reduces the risk of errors in role assignments, improves compliance, and ensures that users are granted the appropriate level of access according to security policies. Additionally, a clear naming convention enhances auditability, allowing for better tracking

of role changes and ensuring that the SAP system remains secure and compliant with internal and external regulations.

The collaboration and communication between the IT and Business departments is smoother when the naming convention is defined, followed and clear. Moreover, consistent naming conventions make role maintenance easier, leading to overall better system management. (Chuprunov, 2013).

For the technical role name letters of Latin alphabet, numbers and several signs are allowed to be used by the system. The maximum limit for the technical role name, defined by the system, is 33 digits.

SAP shares best practices and recommendations of an option how the naming convention can be defined for the SAP roles, Spaces and Pages. The purpose of usage naming convention is reflected in the accelerator, as well as key aspects, which might be reflected in the roles', spaces' and pages' names. From the technical point of view there is no restrictions for the naming convention, in spite digits and signs limitation, described in the previous paragraph. Otherwise, the naming convention is designed by each company individually, based on, for example, requirements for the potential role analysis (SAP, 2024).

2.5 Critical Authorization Objects

SAP critical authorization objects are specific elements in the SAP security model that represent highly sensitive or impactful functions or data that require strict control. These objects facilitate particular actions within the SAP system that, if improperly authorized, could lead to significant security risks, like fraud or data breaches. Because of their potential impact, these authorization objects require careful oversight and management to ensure that only appropriately privileged and verified users have access to them. For example, an authorization object could control the ability to transfer funds, adjust

master data for vendors or customers, or change configuration settings that would affect on the operation of the SAP system. A thorough understanding and analysis of these objects are crucial for establishing a secure SAP environment, as reflected in a complete analysis of the most critical authorization objects to prevent fraud and ensure compliance with various regulations (González, 2016).

Authorization objects are used in SAP to protect functions or data by combining them with action values to define specific permissions. When a transaction is executed that checks an authorization object, the SAP system verifies that the user has the required permission for all the authorization fields of the object (Lamotte-Schubert & Weidenbach, 2009; Lamotte-Schubert, 2015).

Furthermore, within the context of General Data Protection Regulation, identifying which authorization objects interact with personally identifiable information becomes critical to ensure compliance. Companies must define these objects clearly within SAP authorizations to address GDPR risk assessments (Mast, 2018).

The management of these critical authorization objects is carried out through user roles and profiles while ensuring that the concept of segregation of duties is maintained to minimize the risk of fraud or error within the system. (González, 2016).

Understanding what constitutes a critical authorization object within your SAP system can vary depending on the business processes, data sensitivity, and specific industry regulations that apply to your organization. Therefore, it is essential for IT administrators to have a strategy for managing these critical objects comprehensively and judiciously. In sum, critical authorization objects in SAP are key to maintain the integrity and security of the system and require special attention to ensure that access is governed appropriately (Hirao & Wun-Young, 2009).

While the exact list of critical authorization objects may vary depending on the specific business processes and industry regulations, some examples are documented in the below table, based on the literature sources of Gallegos & Tison-Dualan, 1999 and Little & Best, 2003.

Table 1. Critical Authorization Objects. (Gallegos & Tison-Dualan, 1999; Little & Best, 2003).

Authorization Object	Purpose
S_TCODE	The object controls access to the transaction codes.
S_PROGRAM	The object controls access to specific ABAP programs.
S_TABU_NAM	This object manages access to specific table entries.
S_USER_GRP	This object manages access to user master records.
S_USER_AUT	This authorization object controls access to user authorizations.
S_USER_PRO	This object manages access to user profiles.
S_RFC	This object manages access to remote function calls.
S_ADMI_FCD	This authorization object controls access to system authorizations.

2.6 Principle of Least Privilege (PoLP)

One of the Security Engineering Principles is Principle of Least Privilege (PoLP), which declares that the user should have access to the applications, data or resources, which are necessary to complete their daily work tasks. Application of PoLP limits the scope of user's actions so that in case of corruption or failure it will cause minimum security consequences or damages as well as make security analysis fairly simple. PoLP is commonly utilized in design of the secure system. Other aspects of the principle are to implement only necessary modules for functioning of the required components and limit access to maintenance activities for the users (such as create, change, write). Only users who really need to maintain something in the system should have access to do it (National Institute of Standards and Technology [NIST], 2020).

To reduce complexity and costs for security analysis it is advisable to include minimum required components. In case if there are too many components for which complex relationships are set, it becomes more difficult to ensure that the system is secured enough. However simpler system, which consists of less trusted components and trust relationships between them are minimized is easily amendable to the security analysis (National Institute of Standards and Technology [NIST], 2020).

2.7 Change and Transport System (CTS)

The core instrument for managing changes in the SAP ABAB Workbench and IMG is Change and Transport System. SAP records all changes applied to programs or system configurations in the CTS. Changes to repository objects managed in the CTS are applied in all clients, nevertheless it is possible to make client specific developments and transport them just to the appropriate clients. CTS records all applied changes in the Change Requests. There is a possibility to link the changes between each other or make independent changes. One change is like a small project on which several developers may work. The changes are captured in the Transport Requests, which are used for copying or transporting the changes from one system client to another. During CTS configuration it is possible to set the rules for the configuration landscape, one of the rules which is frequently used is that all changes must go through the test environment and carefully tested before they are transported to productive system. Following this rule reduces the risk of production breaks. Usually, the change is developed in the development client, transported to the test client and after successful testing moved to the productive system (SAP, 2024).

Before the company starts using CTS, it should be adapted to company's business requirements and needs. This process is continuous and lasts also after the go-live, for example, due to organizational changes or need of implementation of other SAP modules. Working in the development project requires usage of Transport Organizer. One of

the important prerequisites for the user is to have specific authorizations (Table 2) (SAP, 2024).

Table 2. Authorization for using CTS (SAP, 2024).

Profile	User type (global view)	Functions in the CTS
S_A.SYSTEM	System administrator (superuser)	**System administrator**
S_A.ADMIN	Operator	Display only
S_A.CUSTOMIZ	Customizer	**Project manager**
S_A.DEVELOP	Developer	**Developer**
S_A.USER	User	Display only
S_A.SHOW	Basis: Display only	Display only

2.8 SAP licensing concept

SAP grants permission to use its software via licensing. Each customer of SAP is responsible for license assignment and management by itself. Therefore, it is customer's obligation to perform yearly SAP License Audit for the SAP. As a result of such audit the client company finds out the amount of active SAP users in comparison with the purchased licenses (SAP, 2022).

2.9 Total Cost of Ownership (TCO) of ERP system

According to Ellram (1995), Total Cost of Ownership includes a lot of purchase-related costs besides the purchase price. (Ellram, 1995).

Major aspects of SAP Total Cost of Ownership (TCO) Include:

- Implementation Costs. SAP implementation projects typically include significant financial investments. Around 60% of the project costs are associated with

implementation efforts. Customization to ensure a 'fit-for-purpose' solution may incur additional costs. (Francalanci, 2021).

- Cost optimization strategies. Organizations focus on keeping SAP environments cost-effective and agile. Cost optimization strategies include System Consolidation (“one SAP”), Cloud Migration, Reducing System complexity. (Bauer & Siebert, 2010).
- Financial Considerations. TCO model helps organizations understand comprehensive SAP-related expenses, including costs beyond the implementation scope: system maintenance, customization, upgrade, trainings and infrastructure. (Bauer & Siebert, 2010).

Complexity and cost reduction. Reducing system complexity can help manage total costs. Unified solutions can reduce total cost of ownership, especially when considering international accounting requirements. (Dijke & Scheele, 2013, p.36-40).

In the article “A Structured Approach to Reducing SAP Complexity” Ad van Dijke and Rob Scheele tell about the attempts of the enterprises to reduce the Total Cost of Ownership by unification of the systems to, for example, One SAP, usage of SAP Cloud system, hiring third party for provisioning technical and functional support. They claim that these attempts did not lead to large and stable cost savings due to high complexity: long way before actual implementation of the change in the system, a lot of customized content, as ABAP code and country specific requirements and manual work, which should be done by the business users. Usage of additional SAP modules, SAP application servers, not cleaned up but migrated legacy systems, outsourcing of the essential part to the external third parties, usage of global SAP environment with local configurations, the growing quantity of outdated interfaces and SAP servers due to mergers and acquisitions. Ad van Dijke and Rob Scheele emphasize that cost effectiveness for usage of SAP by the enterprises can be reached by lowering the complexity. Authors’ approach on the analysis and reduction of the complexity is reflected in the article. (Dijke & Scheele, 2013, p.36-40).

The authors give definition of the “Complexity” and list the characteristics, which may influence on the complexity of the system. Some of these characteristics are amount of the subsystems, interaction and operation between the systems, diversity (as different posting types) and demands. There are two types of the complexity: Controlled (Manageable or Rewarded) complexity and Unrewarded complexity. “Rewarded complexity is complexity that adds business value.” (Dijke & Scheele, 2013, p.37). This complexity type is counted a sustainable and manageable. Product, organizational and process complexity are related to the Business Complexity. Business complexity factors reflect and are reflected by the Rewarded complexity of the SAP system. Authors defined five categories of the Rewarded, SAP complexity, which are the Transactional and Master data processes, Interfaces, Landscape and Customized Developments. Several examples of Unrewarded complexity in SAP are reliability on the external consultants with the specific knowledge, complexity of the organizational structure, high number of the customized developments, time consuming workflow from initiation until implementation of the changes in the system, etc. (Dijke & Scheele, 2013, p.36-40).

Designing of the complexity reduction program can be done based on the outcomes of the analysis of SAP system complexity. Analysis of complexity are done in 3 steps. First step is to make an assumption of the complexity factors. It is done by investigating the system, observing documentation and performing interviews with colleagues and partners. The second step presumes measurement of SAP complexity comparing to standard SAP version, paying attention to customizing, customized developments, deviations from the standard business processes, etc. As a result of the third step, complexity factors and opportunities for complexity reduction are identified. As a next step authors propose to determine the scope of the complexity reduction program – they provide examples of the actions which might be included. In conclusion, Ad van Dijke and Rob Scheele believe that the enterprises that properly manage complexity of their SAP system, have a benefit of cost efficiency. (Dijke & Scheele, 2013, p.36-40).

In the article “Evaluating Total Cost of Ownership for University Enterprise Resource Planning: Case of Maseno University” written by Mr. Owoche et al. there were presented the results for the TCO for the Microsoft Dynamics software, which have been implemented by Maseno University in 2007-2008. On the moment of implementation, it was the latest available version of Microsoft Dynamics - ERP system for small and mid-sized enterprises. University’s selection was on-premise software version. TCO calculations included Procurement Costs, Hardware and Software, Implementation Costs, Operations and Maintenance Costs and the costs for the End-User Usage. TCO for the ERP system of Maseno University has been calculated used modified Gartner’s TCO model. Calculations are reflected in the table 3. Figure 3 in its turn visualizes ERP TCO in the percentage ratio. According to this bar chart Operations and Maintenance costs cover 51% of the whole TCO, including most expensive procedures: Maintenance and Support, what is visible from the table 3. Only 3% of whole TCO has been assigned to the Software Procurement Costs, which include Feasibility Studies, Requirement Specification, Procurement and Project Management. According to Gartner’s theory, initial acquisition cost for the ERP software does not exceed 20% of the TCO and in this article the authors point out that the Software, Hardware (16%) and Procurement costs (3%) are 19% of the whole TCO. The rest 81% of TCO is under control of the university, what means it can be optimized by applying sound management practices. (Owoche et al., 2015, p. 79-87).

Table 3. Five Year TCO of Maseno University ERP System (Source: Research data) (Owoche et al., 2015, p. 84).

	Nodes Costs (KES)	Elements Costs (KES)
Procurement Costs		3,300,000 **(3%)**
Feasibility Study	800,000	
Requirement Specification	300,000	
Procurement Management	1,000,000	
Project Management	1,200,000	
Hardware/Software		20,175,600 **(16%)**
Application Software	3,249,000	
System Software	8,476,600	
Hardware	8,450,000	
Implementation Costs		9,541,572 **(7%)**
Technical Setup	8,281,572	
Change Management	200,000	
Personnel Restructuring	400,000	
Testing	60,000	
Training	600,000	
Operations and Maintenance Costs		66,324,720 **(51%)**
Licenses Agreement	925,000	
Overheads	4,527,063	
Maintenance	31,500,000	
Support	28,672,657	
Monitoring	300,000	
Upgrade	400,000	
End-User Usage		29,735,346 **(23%)**
End-user Operations	5,786,604	
Downtime	23,948,742	
Total	129,077,238	

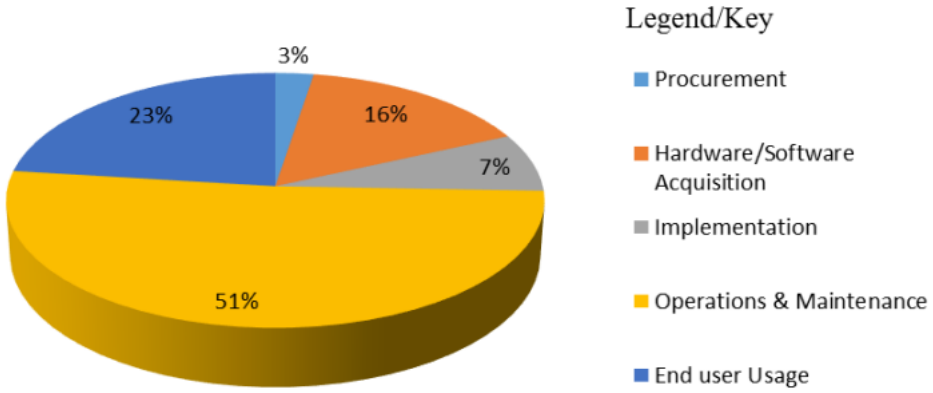


Figure 3. Five years TCO of Maseno University ERP System (Source: Research data) (Owoche et al., 2015, p. 85).

Another case study of Palmberg N. and Göran R. includes analysis of the elements affected on customer expenditures during implementations. It is highlighted that the expectations should be established and the scope clearly defined. Contracts between

vendor and customer should be clear and understandable in the same way by both sides. It is important for the vendor to give realistic estimate of work volume to the customer already in the very beginning. Incorrect definition of the workload might lead to project delays, large budget exceeds and, as a result, client's dissatisfaction. So since the early phase of the project, it is essential to have transparent and frank communication between the vendor and the customer. Also, it is important to mention that the customers should remember about the opportunity to benefit by being strong enough during the negotiations with vendor (Palmberg & Rydgård, 2010).

Palmberg N. and Göran R. designed TCO model in their thesis work, which could be useful for future evaluations of project implementations, including framework of defining the costs and methods of how these costs could be found. It must be emphasized that project controlling and follow up should be improved by having regular meetings between the steering group with representatives from both parties. It is worth noting that the during the study the authors found out an advantage of the customer to have an experienced project manager. The proposed option is to hire project manager from the outside of the organization (if there is no experienced in-house professional). Central purpose of this to save consultancy and internal employees' working hours (Palmberg & Rydgård, 2010).

This research also suggests sticking to the standard settings as much as possible, in order to save the money for both vendor and customer. As a result, customer might have to spend the extra costs for adjusting its business processes to the system, but these costs are more than compensated by the savings on customizing costs. Another issue that customers usually do not register internal times, which brings up the difficulty of tracing expenses of associated costs (Palmberg & Rydgård, 2010).

3 Research Methodology

The research method selected for this study is mixed method approach. A mixed method approach refers to the systematic integration of both qualitative and quantitative research methods within a single study. In this research it allows the combination of numerical data with in-depth contextual insights to obtain a more comprehensive understanding of the phenomenon.

This chapter outlines mixed method research design employed in the present study. The empirical component of the mixed-method approach is based on data extracted from the currently used SAP ERP productive system, enabling the analysis of real operational records within the organizational content. Complementing this, the qualitative dimension of the study is grounded in a comprehensive literature review and observation of existing authorization maintenance process, as well as the process applying authorization changes during the project of transitioning to new SAP S/4HANA ERP system. This provides the theoretical framework and supports the interpretation of the empirical findings. Together these methodological components offer a robust and integrated basis for addressing the research objectives.

The combination of these methods allowed for triangulation of findings and ensured a deeper contextual understanding of authorization and license management practices. The overall purpose of this methodological approach was to generate sufficient evidence to address the three research questions guiding the study.

3.1 Numerical data

During the study the data used for the mixed method research has been retrieved from currently used SAP ERP Productive system: VHP. Ten data sets have been exported and based on them the data for the research was prepared. One data set consists of the list of technical user IDs with X number of days since last log on to the VHP system.

The data used for the research is total amount of the Dialog active users for each month and delta, which represents the difference between the amount of unused user accounts comparing to the previous month. User list for one month has been exported from the system by accessing User Information System in transaction code SUIM, selecting “Users”, then click on “By log on Date and Password Change” and enter the search criteria 300 for “No. days since last logon”, making selection for valid and Dialog users (see details in Appendix 1). After the selections are made, execute and export user data. Repeat same steps for number of days: 270, 240, 210, 180, 150, 120, 90, 60, 30. Considering that there are 30 days in month, as a result data sets for 10 months are gathered.

Calculations for the next step are reflected in the Appendix 2. Table consists of the columns: Period, Days since last logon to the VHP system, Amount of users who have not logged in to VHP, Delta: Amount of users who have not logged in to the VHP since previous month. Amount of users who have not logged in to VHP is the number of users from the exported earlier ten files for each month respectively. Delta: Amount of users who have not logged in to the SAP ERP Productive system since previous month is calculated by the formula:

$$A = delta\ B, \qquad (1)$$

where:
[A – Amount of users who have not logged in to the SAP ERP Productive system since some specific time/month;
delta B – Difference between amount of users who have not logged in to the SAP ERP Productive system for the selected month and the users, who have not logged in to the SAP ERP Productive system for the previous month, than the selected one].

Initially it was planned to exclude the users, who uses Fiori Productive system, from the data sets retrieved from the SAP Productive system. But during the process of data

cleaning, it was decided not to consider usage of Fiori Productive system. The details can be found under 1.4 Limitations.

Data for the previous months has not been used as last time user deactivation was done in VHP in beginning of October 2023 for the users who has never logged in or logged in earlier than 3 months from the date of deactivation; excluding newly created users and only Fiori Users. Note that the users are not removed from the system completely but deactivated by setting valid through date, removing roles, profiles and license data.

3.2 Data analysis

For the data analysis central tendency measures of descriptive statistics: mean, mode, median were applied.

Mean is calculated by the below formula:

$$Mean = Sum\ of\ the\ data\ for\ 9\ months\ /\ 9$$

$$Mean = (12 + 4 + 16 + 14 + 15 + 11 + 19 + 34 + 79)/9 = 22,67 \approx 23.$$

Mode is the most common number, which appears along the number set. Therefore, it cannot be defined for this data set as there is no duplicates: 12, 4, 16, 14, 15, 11, 19, 34, 79.

The amount of values in the dataset, used for the analysis, is 9 which is odd. To calculate Median for odd data set the numbers should be arranged in the ascending order, apply below formular, which will help to identify middle element.

$$Median = (n+1)/2$$

where:

[M – Median;

n – number of elements in the dataset].

Median was calculated as:

Arrangement of data elements in ascending order and applying below formular: 4, 11, 12, 14, 15, 16, 19, 34, 79.

$$M = (9+1)/2 = 5.$$

The Median is 5th element, which is **15**.

3.3 Interpretation

In order to find out where the middle of numerical data distribution lies the measures of central tendency have been used and results reflected under 3.3.2. Data analysis. After the calculations the result was the following: Mean = 23; Mode = not applicable to the data set; Median = 15.

Mean is an arithmetic average, which is efficient in statistical sense but vulnerable to outliers. The smallest value in our data set is 4 and the highest is 79, so there is quite a large delta between the smallest and the highest number. Median in its turn is less affected by the outliers than mean, which makes the median a better choice for the variables with the large number of outliers. Due to the layoffs there is higher amount of inactive users in February and March 2024, which can be assumed as outliers in our data set. Median amount of users is 15.

The mean is 23, which indicates that each month in average 23 new users become inactive comparing to the previous month. It will cause different expenses depending on the license type, assigned to inactive user. After observing the forums, it can be concluded that most frequently used periods for user deactivation is 6 or 12 month. From another

side, companies, who want to cut the costs, might decide to make user deactivation most frequently but should take into account the workload of potential requirement for user reactivation. It is also critical to take into consideration that some of the users have to log in to the system for the small tasks every day, but others use SAP rarely also depending on their tasks.

In addition, by the growing amount of user who have not logged in to the system comparing to the predecessor month, it can be concluded that amount of inactive users is always increasing. If it would go to negative value, it would mean that inactive users from the previous month became active or amount to new active users exceeds calculated delta of inactive users between current and predecessor month; but this is not the case in this research.

3.4 TCO – what is it with software cost analysis

Total Cost of Ownership is the overall cost of acquiring a product, in our case – S/4HANA system, including purchasing, operational and maintenance costs over its lifecycle. During the process of conducting this study there has been created a list of cost elements, which could be utilized for TCO calculations.

In the case of VA, costs incurred in the project consist of the workload of internal and external personnel, which currently presented in company's balance sheet as an asset. As final SAP user roles (Composite roles) are not defined, license contract has not yet been concluded and the cost elements for TCO calculation are currently expressed in the work hours spent, there is not enough information for TCO calculation based on cost elements listed in Figure 4. Therefore, TCO which is based on the Cost Elements for the Software program has not been calculated for this thesis.

Considering that the project for transitioning to the S/4HANA system has been temporarily put on hold, there are two possible outcomes: that project continuation will or will

not take place. If the system is implemented, after the implementation spent costs will be recognized in profit and loss through depreciation divided equally to the lifetime of the system (in our case it would be 10 years). If the implementation does not take place, spent costs will be immediately recognized in profit & loss as an impairment.

In the case of Valmet Automotive the selection fell on deployment of the software on the private cloud, on premise, when company owns full responsibility for the IT management. In terms of cost savings other deployment options could be considered.

	TCO for SAP S/4HANA
	Cost element
≤ 20% of whole TCO	**Procurement costs**
	Feasibility Study
	Requirement Specification
	Procurement Management
	Project Management
	One-time SAP license purchase fee
	Fees for additional functionalities/SAP modules (EWM, TM, YL, iPPE)
	Third party software (costs for integration with third party software&licenses)
	Hardware/Software
	Application Software
	System Software
	Hardware
	Implementation Costs (project management, customization, data migration)
	Integration costs with third party software
	APIs and Middlewear: Costs for integration tools and ongoing support.
	Technical Setup
	Change Management
	Personnel Restructuring
	Testing
	IT Team Training
	Operational and Maintenance Costs
	Salaries for ERP administrators and support team
	Customization
	Custom developments (Z* transactions, reports, etc)
	Regular license costs (yearly)
	Overheads
	Maintenance Fees (vendor support and maintenance agreements)
	Support
	Monitoring
	Upgrade
	Security management (Firewalls, encryption and monitoring services)
	End-user training(continuous training for new features and updates)
	Stakeholder engagement: Initiatives to ensure smooth adoption.
	End-User Usage
	End-user Operations
	Downtime during implementation
	Impact of replacing existing system
	Total

Figure 4. List of Cost Elements for definition of the TCO of the S/4HANA project.

4 Research findings

This chapter includes research findings and answers to the research questions.
Research questions are:

1. How is SAP role maintenance done?
2. What is the process of transporting the change made for the SAP role to the productive system?
3. How to minimize costs for the SAP licenses and what should be done to keep them on the minimum level after go-live?

4.1 Role maintenance and Transport in SAP system

Research question related to the role changes has been addressed by the company for definition of the steps needed for the role maintenance in SAP S/4HANA system after the Go-Live.

After the End user is facing with the authorization error, the Key User should document the error/request for the changes in the role in the ticket for the IT department, which is later assigned to the Authorization Specialist. Authorization Specialist should check if the there is enough data for fixing of authorization error and request more information if needed: usually SU53 report and screenshot of the error message are necessary for analyzing the error and defining if it is related to the authorizations. Meeting with Key and End Users is organized for replication of the error, if needed. Change request is created in Solution Manager by the Authorization Specialist for which Transport Requests are created. Changes are captured in the TRs.

After performing the literature review and as a result of the observation of the currently used processes for the role maintenance in addition to processes used during the project if transitioning to the new SAP ERP S/4HANA system, it was discussed internally that

initially the change is done in the SAP Development system by the Authorization Specialist:

- Log in to the Development system;
- In case if in the SU53 report the return code is 12, maintenance of the authorization default values in the transaction SU24 is required. The limitations for setting the default values should be documented in the Authorization Concept and followed. Changes are saved in the Workbench Transport Request.
- If the return code for the error is 4 or maintenance of the authorization default values has already been done in SU24 (previous step), authorization values should be maintained in the related role: transaction PFCG.
- In PFCG enter the Technical role name (Changes are always done in the Master role and after distributed to the derived roles. Single and Object roles do not have derivations), click “Edit”, go to tab “Authorizations”, select “Expert Mode for Profile Generation”. Make changes to the unmaintained fields according to the error in the report, requirements from the key user and Authorization Concept Documentation. After the status is maintained and turned to green, the roles’ profiles should be generated. In case of maintenance of the Master role, profiles for the Derived roles should be also generated by clicking “Generate Derived Roles”.
- After that go back to the initial screen of PFCG. Technical role name still remains in the field. Click “Transport”, if you need to transport Single or Object role. If the change was made for the master role, the Derivations must be transported along with the Master role. To transport Master roles with all related derivations click: “More” > “Utilities” > “Mass Transport” and enter all Derivations. It is possible to enter them in one line, in case if naming convention has been defined properly and derivations for one Master role are differentiated by, for example, ending. Parent role is always transported with the Child roles, so it will be automatically captured in the same Customizing Transport Request, as its Derivations. User assignment is not transportable in our case.
- There is additional step for running the task list for activation of OData services, which should not be forgotten in case of adding Fiori App to the role.

- In some cases missing service might cause authorization issues. It will be visible on the SU53 screenshot and required changed done in PFCG.
- Content of Transport Request can be checked in transaction code SE10. In the same transaction the task should be released.
- The task under the Transport Request is released by the Authorization Specialist. After the Transport Request can be transported by the Change Manager to the Quality Assurance system for testing.
- Testing is performed by the Key User in Quality Assurance System. For that Authorization Specialist creates test user, to which proper role(s) is/are assigned. There is also a possibility to create Test users, which Key users might use for role- and other testing. Testing must be documented in the ticket.
- After that change is confirmed by the Key User and CR is approved by the responsible person, the role(s) are transported to the Productive system. After which validation takes place by the Key User with the End User.

4.2 Keeping license costs on the low level

As a result of research, which has been done for this thesis, minimum 4 and maximum 79 users are not using SAP ERP system, comparing to the previous month (see Appendix 2), what highlights the necessity to make regular system reviews to find user accounts, which are not in use during some specific period of time and deactivate them. Common Best Practices, based on industry standards and GDPR Interpretation, refer to 90 days inactivity rule before user deactivation. More security-focused approach is to disable active unused users after 30-60 days of inactivity. Standard ISO 27001 (Annex A.9 – Access control) requires regular license review but does not include mandatory timeframes for it. Finland's NIS2-based cybersecurity regulation requires proper access control and periodic reviews but does not define retention limits; companies handling critical infrastructure may require stricter policies (e.g. 30 days of inactivity limit).

After the internal discussion it became clear that license fee includes one-time license purchase fee and yearly maintenance cost for every purchased license. Basically, user deactivations are done in terms of following that usage of SAP licenses is not exceeded amounts of purchased licenses, agreed in the contract. It is easy to check amount of licenses utilized in the system by performing User Classification in transaction code USMM and compare it to the amounts agreed by the contract. This procedure can be done between user deactivations, for instance - monthly. Alternatively, customized program could be created to make comparison, described in the previous sentence, and if the amount of the licenses has been exceeded listed licenses in the contract, the email with the alarm could be sent to the person, responsible for making user reviews, for doing license check immediately on request to fix the mismatch. Except of initial expenses for development of such customized program, there might be required additional expenses in the future, in case if there will be any changes in license amount in the contract, the program would have to be changed in accordance with them. It could be referred to disadvantage of making this development, as User Classification and license comparison can be done manually as often as needed for the company - it is quite straightforward and does not require a lot of time.

As mentioned in the previous paragraph, residence period for the misused users to stay active in the system should be defined individually by each company, assuming the workload for reactivation and individual task, which might require rare log on (for example users, who use the system for seldom Approval or Purchase Requisition Creation tasks). Another alternative is to conduct “unplanned” user checks, for example after such organizational changes, as layoffs. The advantage of this approach is that it is possible to conduct more or oppositely less user checks during the same period assuming different periods of users’ inactiveness, depending on the situation inside the company. The positive aspect also that the workload of the person, who is making the check, can be distributed, depending on the task’s urgency, when the specific time for performing license check is defined by the company. The disadvantage is that due to the human factor the check might be delayed or forgotten.

It is reflected in the theory part that it is more cost benefit to keep SAP system as simple and close to standard as possible, which adequately meets business requirements. It would be more cost effective in the end to adapt companies' business processes to the standard functionality available in the system. Costs for adaptation of the internal business processes would be much less than expensive for system customization. The idea to not overcomplicate the system is also valid for the area of authorization and authorization concept, it is interpreted in the PoLP: users should have minimum required access to be able to perform their daily work tasks.

What if there are lots of developments done for the SAP role, when role's license type should be changed to the next one in the hierarchy? And how to understand that? In this case there are several aspects, which should be taken into account. First, it is very important to understand the license hierarchy. Higer licenses include wider authorizations and are more expensive. Roles' authorizations should be analyzed in terms of access to critical transactions (such as SU01, SE38, PFCG, etc.), access to create/change/delete master and operational data, ability to only display vs. change data vs. making configurations. In USMM transaction it is possible to map the usage to the license type manually with the help of the licensing guide. There are third party tools (like Snow, VOQUZ, Aspera) for analyzing actual usage patterns in relation to license definition from SAP and which recommend license types per user, show cost savings (for ex. by downgrading licenses), identify conflicting roles vs. assigned licensed types. Steps for manual reviewing the role may include creation of the list with the transaction codes, assigned to the role, which is under consideration, adding the description for each transaction code, activity type (display/create/change/post/delete) and affected data types (Business or Master data) and identify SAP license type, which is covering described actions.

The theory part has been widened while writing the thesis paper to cover not only SAP license costs but also the TCO. Thus, lowering other costs has been also considered in the theory part. It could be done through clear and transparent communication between providers of implementation services and customer with common understanding of the

contract, clearly defined scope on the very beginning stage of the project and correct and close to reality estimation of the workload for the customer. Incorrect definition of the workload might lead to the budget exceed and project delays. It can be concluded that the customer is able to gain cost benefit during the negotiations with the vendor. For definition of potential expenses and workload estimation it is necessary to calculate TCO, which should be under control during the whole project lifecycle – regular meetings between vendor and customer steering groups are expected to be held. Also, the importance of having an experienced project manager has been highlighted: he would lead to savings related to the working hours for both internal and external project parties.

4.3 Validity and reliability of the study

To ensure the reliability of the research results, careful data collection has been done for 10 months in a row with constant data intervals of 30 days, which was considered as a month. Research data has been transparently documented along with the research. It is important to utilize up-to-date and accurate data from the reliable data sources. (Saunders, Lewis, & Thornhill, 2016). In this case the real data have been collected from the valid data source, current Valmet Automotive Oyj SAP ERP system, and consistently transformed along with the research plan. Consistency and detailed description of the criteria for collecting the data guarantee the possibility for other companies for replication of the research with their own data (Saunders, Lewis, & Thornhill, 2016). As stated by Saunders, Lewis, & Thornhill (2016), several important steps are taken in order to confirm the reliability and validity of the data. These steps include a Completeness Check to ensure all crucial data points are included in the dataset without any omissions; a thorough Consistency Check that carefully detects any discrepancies or incongruities in the data; and a thorough Sensitivity Analysis, which give thorough assessment for the strength of the research findings. In addition, the literature review has been made based on the scientific information and all references are included in the reference list.

4.4 Gap analysis for the future research potential

Currently a lot of companies are moving toward usage of ERP SAP S/4HANA system but considering tough times on the market not each of them has resources to implement SAP GRC tool. Of course there are “replications” of this program available, what means less but additional operational costs. It would be useful to make research and open up what are the steps for definition of the SoD conflict in the SAP system with the greenfield approach, prepare a list of critical transaction/authorization object combinations and design a process of how the roles should be reviewed after they affected by the changes. SoD conflict on general (between the SAP roles) and on the Single role level (avoiding conflict combinations of transaction codes inside the single role) are critical and inevitable topics for every company.

4.5 Managerial Implications

Based on the research findings the amount of SAP unused user accounts has been constantly growing during half of the year time period. To shorten the license costs implication of this study suggests accurate follow up and periodic deactivation of inactive users.

Role maintenance process, defined in the Authorization Concept, should be followed along with the path for transporting the changes. Also, it is necessary to document role changes properly.

Another recommendation which comes out from this research is to keep the system as simple as possible by implementing minimum SAP modules, which are required for performing daily work operations.

There are different deployment models, selection of which will affect on company’s operational costs. Deployment model has already been selected by VA but in general and

for other companies, which are going to make an ERP transition, it is advisable to approach deployment model selection carefully.

4.6 How to proceed with Authorizations in SAP S/4HANA?

As Authorization Concept includes Master roles, Single roles and Object roles for non-organizational restrictions, several sets of derivations of the Master roles, it is complex and need to be followed very carefully. Role catalog has to be updated after Authorization related change is made to the role and defined role maintenance steps have to be followed by the Authorization Specialist. Also, other related documentation, linked to the Role Catalog must be always up to date.

Also, it is very important to make key users aware of the general principles of the Authorization Concept and the SAP role design. In the case of Valmet Automotive it should be highlighted that: SAP roles are split into the categories of Display, Master Data Maintenance, Dynamic Data Maintenance, Customizing, critical Roles, e. g. Release or Mass Changes; one transaction should be assigned to only one of the Master role (the exceptions may also apply); Object roles are used for non-organizational restrictions (for example if the user needs to access some specific table or have authorization to some Cost Centre); etc. As an option is to prepare simple overview course or series of courses, which cover principles of authorization concept, with the examples, available on the Success Factors for the employees.

5 Summary

The purpose of this thesis was to define the process for handling authorization errors and changes, its transport through the system landscape and to find the ways for keeping license costs at the low level. The thesis consisted of the literature review for a theoretical part, including implementation of the SAP S/4HANA ERP system and Authorizations, critical authorization objects, importance of following role naming convention, SAP licensing concept and Total Cost of Ownership of the ERP system. For the research question related to the cost savings, analysis of descriptive statistics was applied on the data collected from the productive system. Deployment models and responsibilities between the parties have been outlined so that the companies can see the effect on the operational costs, depending on selection of specific deployment model.

Based on the study and literature review, it was defined that user deactivation of unused user accounts in the SAP ERP system should be periodically done to prevent exceeding the licenses count specified in the contract. Information security principle of least privilege (PoLP) should be followed by limitation of authorizations to essential for the user for performing his daily tasks. It can be done by regular users' access rights reviews. For Valmet Automotive Oyj, as well as for other companies, it is necessary to follow up that the usage of SAP licenses does not exceed the limit of purchased SAP license amount, listed in the contract. Valmet Automotive Oyj has to pay yearly maintenance fee for all purchased licenses recorded in the agreement, nevertheless if they are in use or not. Comparison between the license status in the SAP system vs. available licenses in the contract can be done as described in one of the chapters of this thesis – with the help of USMM transaction code. Procedure of deactivation of unused user accounts prevents company from such expenses, as fines, invoices for the past periods of using licenses without paying for them or higher pricing issued by the license provider party of the contract. For every company potential financial impact of the user deactivation procedure might be different, as the license contract is usually negotiated individually, depending on the selected license model, license types, negotiated license costs, user amount.

As the theoretical part demonstrates, in addition to regular user deactivation process, Cost of Ownership can be kept on the minimum level by reducing complexity of the SAP system and stick to standard settings available in the system. Adjustment of the business processes to program's standard processes would be substantially cheaper than system customizing. Other important aspects, which advisable to take into account by companies participating in ERP transformation, are assurance of having clear agreements understandable in the same manner with the vendor, being aware of clear scope and required workload. Communication between vendor and customer should be transparent and regular since the early project phase. As per one of the case studies listed in theory part, it is advisable to evaluate costs for project implementation by using TCO model prior to the project start and engage professional and experienced project manager in order to save consultancy and internal employees' working hours, what will result in significant savings. Another point which should be highlighted is that internal time registering is unusual occurrence – thus the company faces the difficulty of tracing expenses of associated costs. These costs are crucial, therefore its follow up and correct allocation leads to considerable savings.

With the help of system observation and literature review the process for handling authorization errors and making changes to the SAP roles has been documented in detail as an individual chapter in the authorization concept document and shortly described in the dedicated chapter of this thesis work. The topic of transporting the authorizations has been also opened and covered in the related chapter, based on literature review and processes used during the S/4HANA project.

References

Amazon Web Services. 2025. Riot Games Cuts $10M Annual Infrastructure Costs by Migrating to Amazon EKS. Retrieved 2025-11-13 from: https://aws.amazon.com/solutions/case-studies/riot-games-case-study/

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. https://doi.org/10.1145/1721654.1721672

Banzer, A. (2022). *Authorizations in SAP S/4HANA and SAP Fiori.* Rheinwerk Publishing Inc.

Buecker, A., Chiu, I., Chow, K., Dressler, I., Ferguson, A., Harper, V., Moore, D., Radenkovic, Z., Redding, G., Robinson, J., Schefenacker, S. & Wolfhagen, F. (2012). *Integrating IBM Security and SAP Solutions.* First edition. 2012. Retrieved 2025-06-13 from https://books.google.fi/books?hl=en&id=gO_HAgAAQBAJ&oi=fnd&pg=PP1&dq=Critical+SAP+Authorization+objects&ots=8jaxo9Fi5i&sig=_HdgAAspe3tTIqlKeO7QuoMOAXc&redir_esc=y#v=onepage&q&f=false

Chuprunov, M., (2013). *Auditing and GRC Automation in SAP.* https://doi.org/10.1007/978-3-642-35302-4_6

Dijke, A. v. & Scheele, R. (2013). A Structured Approach to Reducing SAP Complexity. *Compact.* Retrieved 2024-06-15 from https://www.compact.nl/pdf/C-2013-3-Scheele.pdf

Durdu, A. & Tutğaç, A. (2022). Examination of Risks in Management of Software Licenses in Enterprises and Cost-Benefit Analysis. *Bilişim Teknolojileri Dergisi.* DOI: 10.17671/gazibtd.1019869

Ellram, L. M. (1995). Total cost of ownership: An analysis approach for purchasing. *International journal of physical distribution & logistics management.* 25, 4-23. DOI: 10.1108/09600039510099928

Bauer, E. & Siebert, J. (2010). *The SAP General Ledger* (2nd. ed.). SAP PRESS.

Francalanci, C. (2001). Predicting the implementation effort of ERP projects: empirical evidence on SAP/R3. *Journal of Information Technology.* 16, 33–48. https://doi.org/10.1080/02683960010035943

Gallegos, F. & Tison-Dualan, L. (1999). *SAP Implementation and Control.* 1st Edition. https://doi.org/10.1201/9780203710739

Haddara, M. (2012. January). Exploring ERP adoption cost factors. *Journal of Computer Technology and Application,* 3(3), 45-52.

Harrison, D., & Lainhart, M. (2015). *Cloud computing for business: A comprehensive guide to cloud computing and its business applications.* Wiley.

Hirao, J. & Wun-Young, L. (2009). *SAP Security Configuration and Deployment: The IT Administrator's Guide to Best Practices* (1 edition.) Syngress Publishing.

How to Set up a Naming Convention for Business Roles, spaces and Pages in a 3-System-Landscape. (2024). Version 2408. Retrieved 2024-08-25 from https://support.sap.com/content/dam/SAAP/SAP_Activate/S4H_1665%20How%20to%20Set%20Up%20a%20Naming%20Convention%20for%20Business%20Roles%2c%20Spaces%20and%20Pages%20(3-system%20landscape).pdf

Kavis, M. J. (2014). *Architecting the cloud: Design decisions and trade-offs.* Wiley.

Krause, J., Meyer, J., & Müller, H. (2021. April). The economic implications of enterprise software licensing models. *Information Systems Management*, 38(2), 94-107. https://doi.org/10.1080/10580530.2021.1878451

Kulkarni, A. (2019). *SAP S/4HANA Implementation Guide.* SAP Press.

Linkies, M. & Off, F. (2006). *SAP Security and Authorizations.* SAP Press.

Lamotte-Schubert, M. (2015). *Automatic Authorization Analysis* [Doctoral dissertation. Saarland University]. Retrieved: 2025-01-26 from https://publikationen.sulb.uni-saarland.de/bitstream/20.500.11880/26675/1/thesis_final.pdf

Lamotte-Schubert, M., & Weidenbach, C. (2009). Analysis of Authorizations in SAP R/3. *International Workshops on First Order Theorem Proving*. Retrieved: 2024-05-15 from https://ceur-ws.org/Vol-556/paper09.pdf

Liao, H. (2009). Design of SaaS-Based Software Architecture. *Proceedings of the 2009 International Conference on Networked Computing and Advanced Information Management*, pp. 334-338. https://doi.org/10.1109/NISS.2009.46

Little, A. & Best P. J. (2003). A framework for separation of duties in an SAP R/3 environment. *Managerial Auditing Journal.* 18(5), 419-430. https://doi.org/10.1108/02686900310476882

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

Martin, C. C., Bajowala, R. R., Borich, A. B. & Powell, L. R. (2017). *Information Technology Disputes.* Attention SAP Customers: Are You Complying With Your License? Check Before SAP Brings You To Court. *Jenner & Block.* Retrieved 2024-12-03 from: https://www.jenner.com/a/web/mW15KhoRbcrTqgp1kxxAJv/4HRMZQ/170410AttentionSAPCustomersAreYouComplyingWithYourLicenseCheckBeforeSAPBringsYouToCourt.pdf?1492049257

Mast, J. (2018). *SAP authorization concept renewal project and GDPR in Company X* [Master's thesis. Turku University of Applied Sciences]. Theseus. Retrieved 2025-01-15 from: https://www.theseus.fi/bitstream/handle/10024/150575/Mast_Jukka.pdf?sequence=1&isAllowed=y

González, M. S. (2016). Fraud prevention through segregation of duties: authorization model in SAP GRC Access Control. URI: http://hdl.handle.net/10016/23673

Owoche, P. O., Wanyembi, G. & Kilwake, H. J. (2015. March-April). Evaluating Total Cost of Ownership for University Enterprise Resource Planning: Case of Maseno University. *IOSR Journal of Computer Engineering*. 17 (2),V, 79-87.

Osaci, M., Cristea, A. D., Ghiuzan, D., & Berdie, D. A. (2018). SAP authorization based on the four eyes principle. *Annals of Faculty Engineering Hunedoara, International Journal of Engineering*. 16(2), 43-46.

Palmberg, N., & Rydgård, G. (2010). *Assessing the total cost of ownership of ERP systems: Case study analysis on the factors behind customer costs in recent minor implementations* [Master's thesis, Linköping University]. Retrieved 2024-11-05 from https://www.diva-portal.org/smash/get/diva2:326335/FULLTEXT01.pdf

Pattanayak, S. (2017). *Real-Time Analytics with SAP HANA*. Packt Publishing.

SAP LeanIX. (n.d.). *S/4HANA: Greenfield vs. Brownfield approach—Greenfield approach: New implementation.* Retrieved 2024-06-05 from https://www.leanix.net/en/wiki/tech-transformation/s4hana-greenfield-vs-brownfield-approach#greenfield-approach-new-implementation

Rimal, B. P., Choi, E., & Liu, H. (2011). A taxonomy and survey of cloud computing systems. *International Journal of Computer Applications*. 39(9), 6-19. https://doi.org/10.5120/5639-7972

SAP License Management. (2022). Retrieved 2024-07-03 from: https://help.sap.com/saphelp_em700_ehp01/helpdata/en/48/bbd202e3cd35b6e10000000a42189d/content.htm?no_cache=true

Sotomayor, B., Montero, R. S., Llorente, I. M., & Foster, I. (2009). Capacity provisioning for multi-institutional grid and cloud computing. ACM Transactions on Computing for Sustainability (TOCS), 1(1), 1-26. https://doi.org/10.1145/1513510.1513512

Saunders, M., Lewis, P., & Thornhill (2016). Research Methods for Business Students (7th ed.). Edinburg Gate: Pearson Education Limited.

National Institute of Standards and Technology. 2020. *Security and Privacy Controls for Information Systems and Organizations: NIST SP 800-53 Rev. 5*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

Transport Organizer (BC-CTS-ORG) retrieved 2024-09-13 from https://help.sap.com/saphelp_em700_ehp01/helpdata/en/57/38dd4e4eb711d182bf0000e829fbfe/frameset.htm

Statista. (2024). Top cloud infrastructure as a service providers. *Statista.* https://www.statista.com/statistics/1383907/top-cloud-infrastructure-as-a-service-providers/#statisticContainer

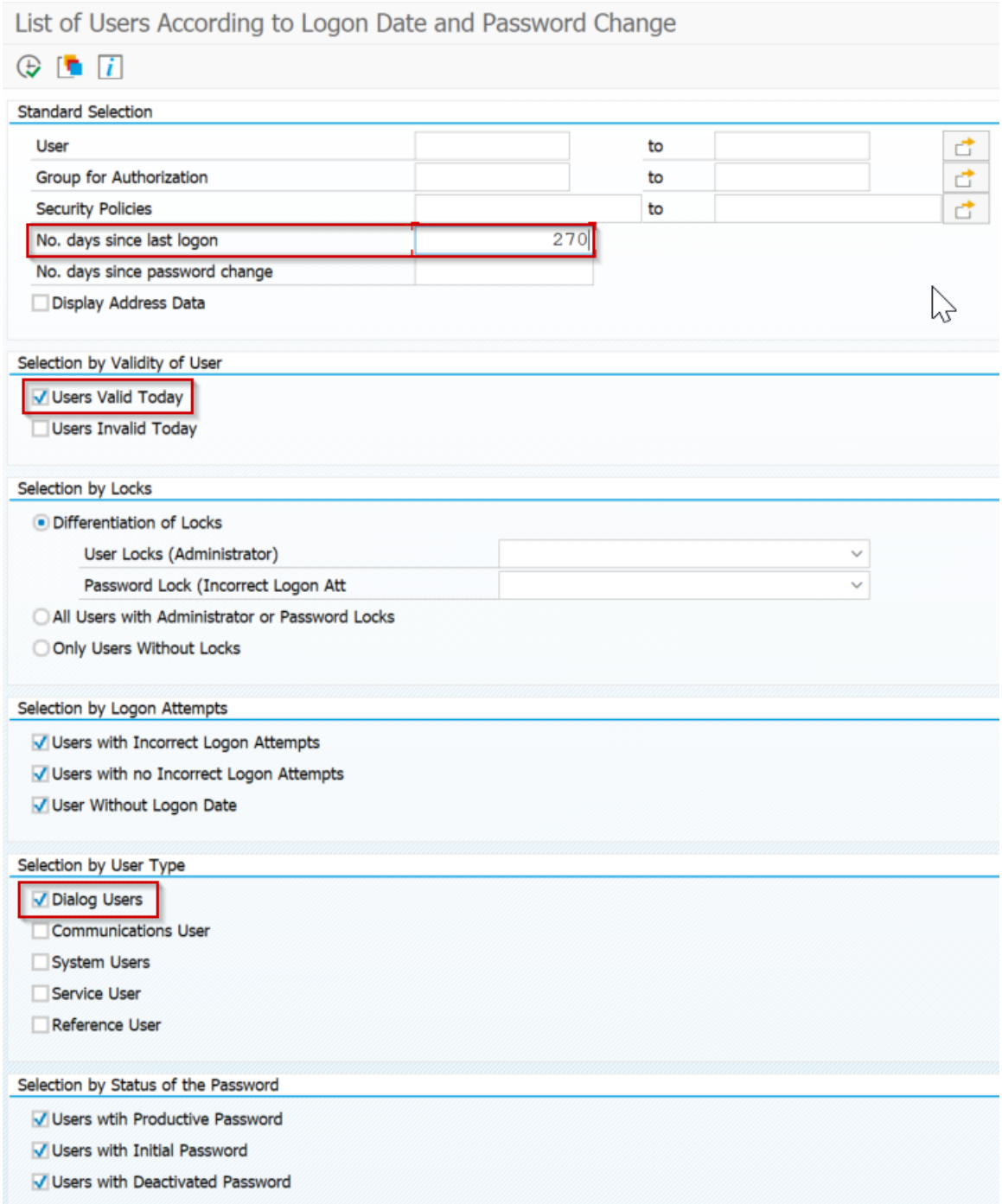
Velkoski G., Simjanoska M., Ristov S. & Gusev M. (2014). In *Proceedings of the SMEs Development and Innovation: Building Competitive Future of SEE.* 801-808.

Wintersgill, N., Stalnaker, T., Heymann, L. A., Chaparro, O. & Poshyvanyk, D. (2024). The law doesn't work like a computer: Exploring software licensing issues faced by legal practitioners. *SSRN*. https://doi.org/10.2139/ssrn.4901954

Zhang, L., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*. 1(1), 7-18. https://doi.org/10.1007/s13174-010-0007-6

Appendices

Appendix 1. Search criteria for the data set (transaction SUIM – User Information System)



Appendix 2. Data set for the research: Amount of users who did not log in since previous month

Period	Days since last logon to the VHP system	Amount of users, who have not logged in to VHP system during set period of time	Delta: Amount of users who did not log in since previous month
Jun-2023	300	99	n/a
Jul-2023	270	111	12
Aug-2023	240	115	4
Sep-2023	210	131	16
Oct-2023	180	145	14
Nov-2023	150	160	15
Dec-2023	120	171	11
Jan-2024	90	190	19
Feb-2024	60	224	34
Mar-2024	30	303	79