Haaga-Helia
University of Applied Sciences

Impact of corporate audit findings on the planning and implementation of SAP ERP Segregation of Duties in a corporate environment

Felix Bloch

Bachelor's Thesis
Degree Programme in Business Information Technology
2020

Haaga-Helia
University of Applied Sciences

Abstract

23 November 2020

Author
Felix Bloch

Degree programme
Business Information Technology

Report/thesis title
Impact of corporate audit findings on the planning and implementation of SAP ERP Segregation of Duties in a corporate environment

Number of pages and appendix pages
25 + 2(15)

Companies worldwide are employing ERP systems such as SAP ERP for their day to day operations. Large businesses conduct regular external and internal corporate audits to examine and evaluate their financial statements which includes their IT infrastructure. To ensure a smooth workflow free of threads which could compromise the system, a proper segregation of duties is required.

This thesis aims to expose the impact of corporate audit findings regarding the segregation of duties on a corporate SAP ERP environment. The focus lays on the implementation project of new segregation of duties within such a system. The goal is to help Wien Energie GmbH to execute future SoD project on their different systems, while also helping companies understand and develop their own segregation of duties.

This paper will first present the company where the project was carried out. Further the reader will be familiarized on the topic of segregation of duties and the environment where the project is executed on. Following, the project itself and the implementation process of are presented. Finally, the obstacles are explained, the results of the project are described and a recommendation for the future is made. Topics such as processes outside of Wien Energie GmbH and interviews with employees are not discussed as they are either not relevant to the thesis.

The segregation of duties was successfully implemented into the SAP ERP system of Wien Energie GmbH. It follows the four-eyes principle which ensures safe operations of the system in the future years.

Keywords
SoD, SAP, ERP

Table of contents

1 Introduction

For decades businesses of all industries and sizes have been employing ERP solutions as the backbone of their operations. Integrated into these enormous systems are sensitive components such as finances or key processes such as sales and distribution. A crucial part of protecting such infrastructures from harm caused by errors, exploitation, and theft is a proper authorizations concept in the form of segregation of duties. Due to segregation of duties, processes are divided in order to be completed and approved by at least two parties. As a result, no single person in a company may hold excess control and power within a closed system. One of the leading ERP software providers is SAP. The company has pioneered ERP software and has dominated the market since the 1980s. SAP ERP systems are complex infrastructures often consisting of thousands of users in different departments, hundreds of roles, and millions of transactions. Thus, the process of creating segregation of duties within such an environment is an exhaustive exercise, which requires a deep level of understanding on the company's workflows and SAP environment.

Wien Energie GmbH is a 100 percent subsidiary of Wiener Stadtwerke GmbH. At the end of 2019, Wien Energie GmbH, the sponsor of this project, had to implement a new SoD concept on request of Wiener Stadtwerke GmbH (WSTW) due to negative corporate audit finding questioning the current segregation of duties (SoD) in their SAP ERP systems. This led to a Wien Energie GmbH internal SoD project. This project is conducted by the IT department. An audit-proof SAP ERP SoD has to be implemented.

The approach to SoD was developed by members of the Demand Management department of Wien Energie GmbH responsible for the needs and project within all departments in regard to IT. The author was as one of the two SAP specialists working on the project. He was part of the IT Demand Management team. Within the project the author was assigned the task to implement the segregation of duties within defined departments. This included the analysis, planning and implementation of SoD for these departments. Further, he was responsible for regularly updating all metadata in relation to all processes.

1.1 Objectives

The overall objectives of this project are to define, test and implement a sustainable and audit-proof SAP ERP SoD solution to each SAP role within each department of Wien Energie GmbH. The results of this project are defined audit-proof SAP roles for all user groups at Wien Energie GmbH and completion of the implementation to the live SAP ERP environment after intensive testing by the alpha users. This goes along with standard documentation of the SoD framework for Wien Energie GmbH.

After the completion of the project, the author will be knowledgeable on the definition of an SAP ERP SoD framework and the corresponding implementation process steps.

1.2 Delimitations

The thesis only discusses the SoD processes outside of Wien Energie GmbH which are performed by members within the IT Demand Management team. This thesis will not discuss any other members of the Wiener Stadtwerke GmbH group or any other company. As they each have developed their own processes on separate systems alien to the SAP ERP environment of Wien Energie GmbH.

Interviews and discussions conducted with key employees of various departments at Wien Energie GmbH are not shared in this paper as these contained critical information and information relevant to the project but not to the thesis.

1.3 Methods

As dedicated project with a defined scope (appendix 1) as well as governance structure have been initiated following the waterfall logic.

The waterfall steps include an as-is assessment, the development of a to-be concept, the execution of the rollout planning, testing and continuous governance of the SoD within the system. Each department is planned in a chronological manner starting with smaller departments proceeding with size. For each department, the steps of the rollout process are conducted one after another, with each composite role being planned in the order of importance. Starting with the general composite role within the department or sub-team, followed by additionally required composite roles such as administration or special teams.

1.4 Wien Energie GmbH

With over two million customers and a yearly revenue of almost 1.7 billion Euros in 2019, Wien Energie GmbH is the largest energy provider in Austria. The company employs over 2100 people and is part of the Wiener Stadtwerke GmbH, which is the municipal infrastructure service provider of Vienna and is owned by the city of Vienna. (Wien Energie GmbH, 2020)

Wien Energie GmbH offers a broad spectrum of products, including electricity, heating, and cooling with an expanding selection of renewable sources. (Wien Energie GmbH, 2020) Further, the company is expanding its business to electromobility, operating the

densest e-charging network in Austria, and telecommunication. The energy is sourced from different types of energy sources with the facilities being located within Vienna and the surrounding area, including the state of Lower-Austria. One of the key energy sources at Wien Energie GmbH is the use of four waste incineration plants such as the Spittelau powerplant. Every year millions of tons of waste produced in Vienna is converted into energy, minimizing the need for landfills and the pollution which results from such depots. (Wien Energie GmbH, 2020) At the same time Wien Energie GmbH puts great efforts into switching renewable energy sources such as solar, wind and water energy. The company aims for renewable energy to make up to 35 percent of their energy production by the year of 2030. (Wien Energie GmbH, 2020)

Wien Energie GmbH uses the SAP ERP Central Component suite, short SAP ECC as their enterprise resource planning system. This system is integrated within all departments of the company and hosts around 1600 users. Projects and demands for the different IT systems and infrastructures at the company are handled by the IT Demand Management department, which acts as an internal consulting team within Wien Energie. The systems themselves are mostly hosted and operated by WienIT GmbH, the IT service provider of the WSTW group. Wien Energie GmbH is also supported by several external partners who contribute knowledge and workforce to the projects. In the past years, major modernization efforts of the IT infrastructure have taken place at Wien Energie GmbH. The goal is to become better connected to the customers with the support of a modern IT environment. New systems and project management frameworks are since being implemented making Wien Energie GmbH a competent competitor on the market.

The implementation of the SoD project was executed by two members of the Demand Management team, with the support of WienIT GmbH on the implementation, and the cooperation of all departments within Wien Energie GmbH to test the new segregation of duties.

1.5 Abbreviations and terms explained

1.5.1 Abbreviations

SoD	Segregation of Duties
RPA	Robotics Process Automation
Q-Gate	Quality gate
SAP	German software corporation
ERP	Enterprise Resource Planning
GRC	Governance, Risk and Compliance

WSTW	Wiener Stadtwerke GmbH
FC	Finance and controlling

1.5.2 Terms

Personal role	A role that has been assigned to an individual user.
Transaction	Code that is used to directly access a program task from the home menu.
Permission	Permissions are included in roles and determine the access of a role.
Organizational unit	“Organizational units are functional units in an enterprise. According to how tasks are divided up within an enterprise, these can be departments, groups or project teams, for example.” (SAP SE, 2020)
Single role	“A single role contains all the authorization objects and field values (organizational and non-organizational) required for the transactions that the role contains.” (Banzer, 2017)
Composite role	“They consist of single roles. Users who are assigned a composite role are automatically assigned the associated single roles during the compare. Composite roles do not themselves contain authorization data.” (SAP SE, 2020)
SAPWorkDir	The work directory for the SAP application located on the user’s system where downloaded files are located.
Firefighter	User which has additional access within a SAP system in case users cannot perform certain transactions. (Kumar, 2020)

2 Theoretical framework

The process of planning and implementing segregation of duties within an enterprise system is a complex process. It consists of several interdependent elements, such as frameworks and tools.

2.1 Segregation of Duties

“A fundamental element of internal control is the maintenance of adequate segregation of duties (SoD), the allocation of work so that an individual cannot both perpetrate and conceal errors or fraud in the normal course of their duties.” (Kobelsky, 2014)

The segregation of duties is an essential part of operating enterprise systems. The goal of segregating duties is the distribution of user permissions based on an authorization concept. The aimed result is to prevent unauthorised access to or abuse of a system, mistakes caused by wrong inputs of data and disproportionate access by external forces.
To achieve the SoD, users must only receive access and the included transactions which are necessary for them to execute their work based on their field/department, position, and responsibilities. Normally, such access is divided and distributed by the use of collections of transactions compiled within user roles. User roles are then applied to organizational units such as leadership, teams, or department groups. As such, each role acts as an administrative unit within a business. (Gehrke, 2020)

The practice of the segregation of duties is abbreviated from the four-eyes principle which is a classical concept of access management and distribution. The four-eyes principle, also called the two-person rule aims to prevent mistakes and abuse of critical operations by separating such into two or more steps which are distributed to be carried out by several people. (Gehrke, 2020) Thus, activities within a system have to be approved by a minimum of two people. This principal comes with cultural change within a company as it enhances authority and monitoring while at the same time improving process performance and efficiency. (United Nations Industrial Development Organization, 2020)

Kobelsky (2014) states, that the segregation of duties greatly differs between the theoretical, pedagogical, and practical literature, auditing standards and the actual practices employed by companies. This is likely due to the lack of theoretical literature on the topic of SoD, while at the same time the practitioner’s models deviating from theoretical literature. The most reasonable cause for this, would be that each business operates differently from the others, as none is the same. Thus, the cases and following the practices are subject to

differentiate within each case, making it impossible to create one or a couple of models for the segregation of duties.

In practice the segregation of duties means that no process within a company may be executable by one single employee. Processes are to be separated into sub processes which are assigned two or more people who have received authorizations based on their duties and seniority level in the company. Activities such as financial, sales and technical operations have to be separated to prevent single employees receiving too much power within a system. (Association of International CPA's, 2020)

2.1.1 SoD-conflicts

“A SoD conflict occurs when a user who is an enterprise’s employee holds excessive permissions in the IT system to be able to perform activities which, from the viewpoint of internal control, security of processes in the firm, good business practices, legal regulations, should be segregated and performed by at least two staff members.” (Szkoda & Cieplik, 2020)

As a result, such conflicts can lead to the abuse of the user’s access rights, data becoming unreliable or unusable due to incorrect handling of the system by inexperience or missing knowledge, and unwanted access by external parties. The segregation of duties minimizes such threads by making it more difficult, but not impossible, for their occurrence to happen and to detect the threads faster and more easily. (Szkoda & Cieplik, 2020)

The most common approach to preventing such conflicts is to not assign combinations of authorization containing SoD conflicts to employees via roles. (Gehrke, 2020) Roles must not contain transactions which when combined cause conflicts with other transactions contained within the role. During the process of planning and rolling out the segregation of duties it is key to analyse the new composite roles for possible new conflicts within the roles.

2.1.2 Authorization

“Authorization is a security mechanism to determine access levels or user/client privileges related to system resources including files, services, computer programs, data and application features. This is the process of granting or denying access to a network resource which allows the user access to various resources based on the user's identity.” (The Economic Times, 2020) Authorizations establish the access of a user depending on their identity and determines if certain functions can be performed. Different users may receive

authorizations on the same object, but their access defines their actions such as read, write or deletion rights. Further the authorizations certify the authenticity of a user on the system.

Authorization objects are a key component of roles within SAP ERP systems which limit a user's operations to the functions assigned to them. Thus, the user receives their authorizations through the roles they are assigned. The user can only access fields in the SAP environment which are contained within the field. (Budhbhatti, 2014)

The segregation of duties is based on the authorization concept of the business and thus crucial for the company to have a strong concept laid out prior to the implementation of SoD. The management and display of authorizations is often assisted by software integrated into a system as it is able to perform analyses at a higher speed and reliability. This provides roles where users receive authorizations that are assigned to them preventing potential misuse of their access rights. During the implementation of SoD authorizations which may cause SoD conflicts are further eliminated so clean roles can be assured. This eliminates further chances of errors in the administration of the authorizations. (Gehrke, 2020)

2.2 Corporate Audit

When talking about audits there are several types of audits used by businesses to examine the state of their financial statements, internal control, and certain processes. The most common types are internal and external audits. An external audit is executed by a certified accounting firm, while an internal audit is commonly done by a team within the business or a hired consulting firm using the standards of the business. (Tuovila, 2020) In April of 2014, the European Commission adopted the legal requirement to certify a company's financial records by the use of an audit. The goal was to improve the reliability of the European markets by giving stake and shareholders a better insight into a company. (European Commission, 2020)

An audit assures that a business meets its objectives and conforms to the common practices and standards. It compares the current state of the subject to the supposed situation in form of standards. The audit analyses the risks and effects of a deviation from the standards and proposes measures and solutions based on the analysis and findings. This recommendation aims to assist the organization to improve the audited object to conform to the practices and standards it is supposed to adhere to. (Petrascu, 2010)

Audits can generally be broken down into several milestones which are conducted spread out over different teams. These milestones are the notification of an audit, the planning process, the initial meeting, fieldwork including constant communication within the auditors and the customer, audit draft, management review & response, exit meeting and audit distribution followed by feedback. (Sisk, 2018)

First, the company is notified about the audit which includes necessary information such as the date and other administrative matters. This is followed by the auditing firm planning the audit to present the scope to the customers leadership during the introductory meeting. During the initial meeting in which the audit is presented, final matters may be discussed. The auditors then proceed with the audit on site, conducting interviews, investigating the systems, and analysing documents relevant to the audit. After the auditors conclude their documentation of the on-site research a draft of the audit document is created and shared within the auditing team to be appended and improved on. Once completed the audit report is shared with the customers leadership which analyses and replies to the findings. After the final exit meeting which informs the auditing firm about the response of the customer, the report is shared with all stake and shareholders to inform them about the findings. Lastly, once the improvements recommended in the audit report are implemented, the customer company sends their feedback on the changes to the auditing firm. (Sisk, 2018)

2.3 Enterprise resource planning

ERP stands for “enterprise resource planning.” ERP software includes programs all core business areas, such as procurement, production, materials management, sales, marketing, finance, and human resources (HR).” (SAP SE, 2020) Together the programs incorporates the different processes within a business and allow free transfer of data between them. This reduces data reduces redundancy and combines all the processes within one core schema. (Oracle, 2020) Through ERP systems different departments within an organization are able to share data and communicate while still using their own software and systems.

ERP solutions are highly individualizable systems that can be moulded around a business’s processes and infrastructures to suit their demands and operations. Such systems integrate all aspects of the company ranging from financial processes, to sales, CRM, manufacturing, supply chain management and many other key operations. When applied properly, an ERP system can contain all processes within a business increasing the collaboration and thus efficiency, reliability, and overview of a business. (Perkins, 2020)

ERP systems are suitable for a wide array of businesses and the systems can be divided into several tiers which depend on the size of a business. (Gehrke 2020, Perkins 2020) Perkins (2020) describes four tiers where tier one is defined as solutions which are suitable for international enterprises, Tier two solutions supply large businesses without a global capacity. The tier three and four solutions are used by mid- and small sized businesses, respectively.

Depending on the size of the company, complexity of the system and software company, the acquisition, implementation, and operation of the ERP solution can be expensive and the most suitable solution including packages has to be selected. The average budget of an ERP project in 2019 was around 9 000 USD per user depending on the size of a company. (Software Path, 2020) The implementation for a tier three and four sized solution may cost between 150 000 to 170 000 USD and for larger businesses the costs can range in the millions. (Peatfield, 2019) Additionally, the yearly costs for maintenance on average costs around 15-20% of the implementation. (Tyndall, 2019)

2.4 SAP SE

SAP SE was founded by former IBM employees in 1972 in the city of Walldorf, Germany as a software intended for data processing. Since then it has grown to be the largest software development company outside North America. (SAP SE, 2020) SAP stands for “Systeme, Anwendungen und Produkte in der Datenverarbeitung” which translates to Systems, Applications, and Products in Data Processing. (SAP SE, 2020) The company reached its status as the principle for ERP during the 1980 when they released SAP R/2 and further extended their dominance on the market in the 1990 with SAP R/3.

SAP SE (2020) states “Traditional business models often decentralize data management, with each business function storing its own operational data in a separate database. This makes it difficult for employees from different business functions to access each other’s information. Furthermore, duplication of data across multiple departments increases IT storage costs and the risk of data errors. By centralizing data management, SAP software provides multiple business functions with a single view of the truth. This helps companies better manage complex business processes by giving employees of different departments easy access to real-time insights across the enterprise. As a result, businesses can accelerate workflows, improve operational efficiency, raise productivity, enhance customer experiences – and ultimately increase profits.”

Currently SAP SE offers a range of software solutions which aim to assist small to large sized businesses with a spectrum of products besides their renowned ERP platforms. In

2019 the company produced a revenue of 27,5 billion euros of which 23 billion consisted of cloud and software revenue. SAP is putting great efforts in expanding their cloud solutions which have increased in revenue by almost 40 percent in 2019. (SAP SE, 2020)

2.4.1 SAP ERP Central Component

The SAP ERP Central Component (SAP ECC) is an on-premises ERP system most commonly used by mid to large sized businesses. The system includes the operations of the different departments of a business within components. The key components most commonly used in an SAP ECC system are financial accounting, controlling, material management and sales and distribution. Further components may be implemented depending on the needs of the company. Additionally, enhancement packages are offered by SAP SE which includes upgrades to existing ECC infrastructures. (Rouse, 2018)

In 2006 SAP SE announced that they would release all new enhancements to SAP ERP as extensions contained in enhancement packages to replace continuous system upgrades with such packages. In the following years, several enhancement packages were released and allowed customers to select the capabilities of their systems. (SAP SE, 2009)

With the release of SAP S/4 HANA in 2015, SAP SE has started with the replacement of SAP ECC as their main ERP product. While company encourages their customers to begin transitioning to the new system and has announced that the support for SAP ECC will continue past 2027. (SAP SE, 2020)

2.4.2 SAP GRC Access Control

The SAP GRC tool is an access control system used to assist organizations with the automatization of the user access management and monitoring processes within their SAP systems. The monitoring feature is a key element of detecting and mitigating SoD conflicts and violations within the system. ”It allows to personalize and customize processes related to users access management, business roles management, analysis and monitoring of the risk of segregation of duties (SoD), privileged / Firefighter access and periodical reviews of access to specific, individual requirements of each enterprise.” (GRC Advisory, 2020)

Regarding the segregation of duties, the GRC system supports the processes by executing integrated risk recognition, risk analysis and continuous compliance within the SAP ERP environment. (SAP PRESS, 2019)

3 Project background

Wiener Stadtwerke GmbH received a group wide negative corporate audit finding by Ernst & Young in regard to a weak segregation of duties within their holding wide SAP environment. Based on the findings and focused on mitigating the issues, they developed holding wide guidelines to be distributed within the WSTW group. Each company within the holding, including Wien Energie GmbH, was tasked to review and update their individual SAP ERP access rights. At Wien Energie GmbH, the project was assigned to the finance and controlling department (FC), which formed a project team consisting of experts from different departments and teams, including the IT Demand Management.

3.1 Wien Energie GmbH As-Is Assessment

After receiving the project assignment/contract, an internal audit of the SAP ERP systems found that the company had neither a clear rule set nor requirements for the distribution of access and duties. Different departments built their own access rights and thus the quality of the access rights depended on a specific department's understanding of the SAP ERP system. This led to almost freely distributed roles and permissions. Users took their SAP access rights with them when transferring between departments and/or hierarchy.

The SAP ERP system was analysed and all transactions within the systems were described and classifier to gain a primary overview of the systems state. Therefore, in the early stages of the project, the project was extended to cover the segregation of duties of all departments, subdepartments and teams of Wien Energie GmbH.

The SAP ERP system of Wien Energie has a total capacity of 2000 SAP licenses. At the project kick-off, around 1600 of the 2100 employees, which makes up around two thirds of the company are housed as users within the SAP environment. The users are divided between the different organizational units within Wien Energie. Such units are contained within teams and sub-teams within each department. The number of organizational units within the SAP environment depends on the size of a department, as well as of its use of the SAP system. The number of organizational units within a department range between five to ten for smaller departments and 40 to over 60 for the larger departments.

Within each department the number of roles varies per team as well as sub-team reflecting the internal structure of the department. E.g. compared to large departments smaller departments and/or teams with limited regular usage of the SAP ERP systems have fever roles assigned within their given structure. Additionally, it might happen that key employees inherit their assigned roles to assistant levels.

3.2 SoD To-Be concept

The project team defined goals as well as non-goals as overall objectives for the project. These objectives have been developed in accordance with the WSTW guidelines and are stated in the project contract. (appendix 1).

3.2.1 Goals & Non-goals

As stated in Appendix 1, page 1, six goals have been defined in total.

- The critical SAP ERP permissions required for regular activities which are process-compliant, are to be covered and approved for all users within all teams and positions without restricting or compromising the efficiency of the operational workflows.
- The SAP ERP permissions of all users are free of any critical permissions that are not approved for the organizational unit of the user.
- The new SAP ERP permissions and roles of all users have to be free from SoD conflicts. Any SoD-conflicts, which cannot be prevented due to organizational reasons, are to be assigned compensating measures.
- SAP ERP permission roles (single and composite roles) which are not used or required anymore are eliminated.
- The firefighter concept, including defined firefighter users and controllers needed for the execution of activities outside the process-compliant activities, are customized/adapted and implemented.

As stated in Appendix 1, page 3, five non-goals have been defined in total.

- Permissions outside the SAP ERP environment and non-critical transactions are considered and adapted.
- Firefighter-user designations, the designation of other types of users or other user groups than in Wien Energie GmbH and permissions of System- and Administrator users are considered and adapted.
- Changes/adaptations related to data protection done by the removal of read permissions are executed and the WSTW rulebook is further developed and expanded.
- The assurance of the compensating measures and the inspection of firefighter activities during ongoing/live operations.
- The governance of the assignment of permissions to the users within Wien Energie GmbH and the adaptation of permission roles during ongoing operations is handled/executed by the IT Demand Management, which permanently ensures the prevention of new SoD conflicts.

3.2.2 Further objectives

In addition to the objectives listed in the project contract, the objectives have been further broken down to describe the project contract in more detail. The extended descriptions of the objectives are listed below.

Permissions within the SAP ERP system are to be reviewed and planned according to the WSTW SAP ERP guidelines for the following processes: financial statement close, asset accounting, and purchase to pay.

Approvers for each above-mentioned process have to be defined in regard to the authorization of critical permissions and compensating measures. Critical permissions are to be determined on the base of which permissions can be applied to which organizational unit.

Compensating measures for SoD conflicts are to be created, as the four-eyes principle has to be guaranteed for all cases where the segregation of duties is not possible or reasonable due to administrative reasons. Compensating measures have to be created with the possibility to be executed on a regular basis. Nevertheless, the risks originating from a SoD conflict may be deliberately/consciously accepted in certain cases.

Users with similar or identical tasks and thus identical permissions within the SAP ERP system are to be included/comprised within each organizational unit. This also includes external collaborators/employees.

A user must only be assigned one composite role, which may consist of multiple single roles. Single roles and individual transactions, which are not assigned to a composite role, may be assigned to a user via a personal after thorough investigation.

The rollout planning is executed through the following steps, which are further described in the following chapter: metadata Update, preparation of the SoD within each department, conflict identification and planning of the SoD within each department, planning of the roles within each department, requesting the implementation, and testing and rollout.

3.3 Rollout planning

The rollout planning is separated into six steps, which have been developed by the team from the IT Demand Management in accordance with the WSTW rulebook. The first step is to update the metadata for the steps to follow, the metadata is collected from the different SAP environments and systems such as the live environment and the GRC system. To make the data collected easier to overlook and work with, this data is stored in several excel files which are stored on the cloud and have the data within the files connected via queries in the rows and tables. Next, the data is prepared so the segregation of duties can be done for each department. As each department is planned individually, all the data necessary for the planning of the department is collected from the metadata files and saved to special excel template forms/files, which were created for the SoD. During this step it is optional to combine existing organizational units into new roles as often times, transactions, and permissions within roles of akin seniority levels, are similar or identical due to streamlined operations within the organization.

After the completion of the data preparation, the first half of the SoD is started by identifying the conflicts within each role of a department. This is done by separating the critical and uncritical transactions within the organizational units as only critical transactions can cause SoD conflicts. This is followed by the planning of the segregation of duties within the department, this is assisted by excel templates which query the data from the metadata files. Once this is completed, the composite and single roles are planned for each organizational unit. A final file is created, which hosts the new composite roles, single roles, and users with individual role assignments on respective pages.
The new roles are free of any SoD conflicts and only hold permissions which are intended for the role itself. Further, the transactions within each role are limited to which have been used before and are needed in the future for streamline operations within the departments. Transactions, which had previously been assigned, but have not been used are removed to limit further risks of SoD conflicts and provide an improved overview of the roles.

After all planning steps have been completed, the document listing the created roles which are now free of SoD conflicts and unfitting permissions is sent to the IT service provider of Wien Energie GmbH. The changes are then added to the system hosting the test environment for inspection by test users within the selected department. Once the testing is completed, pilot users within the live system are assigned the new roles which are then further tested during day to day operations. Finally, the changes are applied to the entire department and the segregation of duties has successfully been completed.

3.4 Schedule

The project contract was first created mid-October of 2019. The contract draws a clear timeline and areas of responsibilities for the project. The first Q-Gate, called Q-Gate 2 was set for the beginning of October 2019. By then, the project initialization and cost-benefit analysis were set to be completed. The next Q-Gate was set for mid-February of 2020 and had the goal of having the project-contract approved. Q-Gate 4 had the target of having the project concept approved by the end of March 2020. The project was set to be completed by the end of July 2020.

The project start was defined as a milestone in which the kick-off within the project team has taken place at the end of Q-Gate 3. The project completion was defined as a milestone following the project handover to the team responsible for SAP operations.

After delays were caused by Covid-19 the planning phase would start mid-May and a new deadline was set to the end of 2020. Due to additional resources, provided due to the addition of an employee in form of an intern from the side of the IT Demand Management, the project was accelerated, and the planning phase would conclude by the beginning of November 2020. Further steps, such as testing and the implementation to the system would commence soon after. This would mostly been in the responsibility of the IT service provide WienIT.

4 Execution of rollout in practice

Prior to the start of the rollout, the team members are trained on the defined rollout process by the use of a training manual (appendix 2), which has been developed in accordance to the WSTW guidelines and the needs of Wien Energie GmbH. The rollout for each department is executed based on the training in order to provide that the segregation of duties is compliant to the defined standards at all time.

The following rollout process has been defined and improved by the Demand Management team based on the findings by EY, guidelines provided by WSTW and their hands-on experience on the system.

4.1 Metadata update

For the planning of the segregation of duties seven key files have to be updated. These files contain the central data for each step within the process. These files have to be regularly updated in order to take already applied and general changes to the system into account. These files are created from the SAP system, with some being processed manually and others using queries with which data is stored into excel files in order to ease the manual planning of the new roles.

4.1.1 Table of users

The first file that is updated regularly, is the table of users which includes the users assigned department. This file contains all users within the organization which are relevant to the SoD planning. These are manually received from the live SAP ECC system.

4.1.2 Table of roles

Following, the table of the user-roles, which contains all existing roles within the organization including the new roles which have been already planned during the SoD process is updated. Again, the data is received from the live ECC system. Here the single-roles and composite Roles are imported into an excel table.

4.1.3 Table of roles with corresponding departments

Third, the table of roles and their corresponding departments has to be updated. This is done within the existing excel file which using automated queries which receive the roles and their assigned departments from the other excel tables.

4.1.4 Transactions in roles

Next, the transactions contained in the roles are received from the live SAP ECC system. In this step, first the SAPWorkDir is emptied, following the single-roles are analogically separated from the composite-roles and then entered into the table. Certain roles have to be eliminated during the process as they are not significant to the process. Finally, all the selected composite roles are saved in the target file using an RPA-process and transferring the results into the table of transactions within the roles.

4.1.5 Analysis file

The analysis file is updated by refreshing the content inside which triggers automated queries receiving the data from the other excel files. This is the largest and most complex file as it contains different views for the connections between all the departments, roles, and transactions. The file is a key element to the planning process and contains extended queries for displaying connections.

4.1.6 Table of transaction usage

The table of the transaction usage data is updated from the production SAP ECC system by a firefighter user and is done for all months. The goal is to have an accurate overview of when the transactions were last used in order to sort out transactions that can be removed from roles during the planning process.

4.1.7 Table of SoD-conflicts

Lastly, the table of SoD-conflicts is updated using the SAP GRC system. Here all the users within the live SAP ECC system are analysed by the system. This is a time-consuming procedure and once completed the results are exported to an excel file.

4.2 Preparation of the SoD within the department

The planning is prepared by the collection of the required data of the department selected for SoD-planning. This is divided into two steps through which the data is collected through a standardized excel document. Depending on the size of the selected department its usage of the SAP system, the document may contain several pages, or the planning is done separately for each team within the department. Optimally, composite roles which can be applied to multiple teams within a department depending on the seniority level and needs are created.

4.2.1 Acquisition of teams including critical transactions

Initially, all users within the selected department and the transactions associated are collected. For this, the users are queried from the table of users. Depending on the size of the department, this is done for each team within the department. Additionally, the transactions used by the users are queried from the analysis file and critical transactions are marked in the document to be further considered throughout the planning. The project team has decided, that only frequently used transactions will be assigned to the new composite roles in order to improve the overview and reduce the risk of SoD-conflicts.

4.2.2 Identification of transactions contained in personal roles

Each transaction is checked for if it originates from a personal role. These roles are marked to be skipped throughout the process. They may be assigned again upon a request but are not to be further considered during the planning phase.

4.3 Conflict identification and planning of the SoD within the department

In this step, the critical and uncritical transactions are entered into their corresponding sections of the SoD planning document. If certain SoD-conflicts have been compensated prior, they are entered into a special section. Once the data has been entered the relevant SoD-conflicts including the causing duties are displayed.

Next, the duties which are not causing SoD-conflicts are combined to improve later overview and simplify access assignment. Each duty fitness to be combined with another duty is evaluated by the use of automated queries determining the possible cause if SoD-conflicts by the combination. This step is iteratively repeated for each duty until all “clean” duties may be combined. Non-combinable duties are further planned manually until each is assigned to a team.

Once all duties have been processed, the applicable transactions are displayed. These transactions are free of SoD-conflicts and are assigned to the users of the team in the following steps.

4.4 Planning of the roles within the department

For each team or sub-team new composite roles and if necessary, single roles have to be planned. The planning is completed once there are no missing transactions left.

4.4.1 Composite roles

Roles in which the previously determined required transactions are contained in, are queried with the help of the analysis file. These roles make up the composite roles which are assigned to the teams. Afterwards, there should not be any missing transactions left besides once that are outdated or seldomly used.

4.4.2 Single roles

In case there are missing transactions which are necessary for a team, a single role containing such, is created. All missing roles are added to the single-role and it is added to the composite role. Single roles may be reused in further composite-roles of other teams.

4.4.3 Inspection

New composite roles are tested to be free of uncompensated SoD conflicts. For this, the new role is entered into a new SoD planning document. After the later implementation in the test environment, the new role is examined in the SAP GRC system and must not display any uncompensated SoD-conflicts.

4.5 Requesting the implementation for the department

A document containing all the prepared data including the new composite role(s), single roles and the corresponding users is created. The document is sent to the IT-service provider to be further processed during the testing and rollout phase.

4.6 Testing and rollout of the changes

A group of or an individual test user is assigned the new composite roles in the SAP test environment and execute extensive tests simulating the work environment. Any problems or other issues are then taken care of using their feedback. Once the testing in the test environment is finished and all problems solved, each team of the department is assigned pilot users. These users use the new composite roles in the live-production system as a final examination of their usability and reliability. After the completion of the pilot phase, the new composite roles are rolled out to all users within the department.

4.7 Improvements to the rollout process

When approaching the challenge of planning and executing the segregation of duties for large departments the hurdle of gaining a preliminary overview arose. Some departments would have up to over 60 organizational units with each team and sub-team often having similar permissions and transactions depending on their duties within the company. The

task of combining similar roles within the departments was thus very tedious and time consuming. To tackle this, a new strategy with the aim of improving and shortening the process a new step in the rollout planning has been developed through the experience gained through the smaller sized departments.

During the analysis of the teams and roles a new excel file is created, in which all transactions within a department are added to the first column of the table. One by one the roles are colour coded depending on their applicability and criticality within the department. Roles which all users within the department may use, are marked green, roles that may need to be further evaluated are marked yellow, roles which may only be given to certain organizational units, often depending on the seniority level, are marked red and any personal role is marked grey to be ignored during further steps.

Following, each organizational unit within the department is added as the header of each column in the first row. For each organizational unit, the roles contained within are marked in the table. This is repeated until each unit has its roles marked on the sheet. A list of combinable organizational units is created based on the similarity of the contained roles to be combined during the further rollout.

5 Obstacles and issues

The project was met with several hurdles which caused setbacks to the process and timeline. The severity differed between each issue, but at no point has there been a thread to the project itself which could have caused it to fail.

The first and most impactful obstacle which has arisen, was one that many businesses had do experience and master during the first half of 2020. In March Covid-19 caused a lockdown for the whole country of Austria. This also affected Wien Energie, as, while it was seen as an essential business which promised to keep all powerplants going, with employees voluntarily isolating at the locations for the duration of the lockdown, all other operations were moved to work from home. (Wien Energie GmbH, 2020) The change to the new work concept proved difficult and many projects experienced delays. The SAP ERP SoD project was no exception, and the project was especially affected as it was meant to start at the end of March. Because of that, the project could not fully commence until mid-May and the planning fully picked up momentum at the beginning of June, when the author joined the efforts/team from the side of the IT Demand Management. The pace was quickly picked up and the new deadline was moved to the end of 2020.

As communication is a critical aspect of the work from home concept, the project was affected by this. The team members lost their ability to interact with each other in the office and key aspects of the project such as onboarding, and training had to be done remotely. To tackle this, Wien Energie GmbH rolled out the Microsoft Office 365 platform to all employees which included the cloud-based services required to be able to efficiently work from home. The project team moved the communication to Microsoft Teams where the members would keep another up to date and discuss progress and obstacles with one another.

A common problem when working on big IT systems with oodles of users, is the communication of change between the executing entity and the end users. This has also been the case on this project, as when presenting the project to key users within different departments of Wien Energie GmbH. Presenting the oncoming changes would cause anxiety for some employees, as the content of the presentations would get too technical and not communicate the actual changes the end user would experience. To combat this, information about the impact of the project would be communicated and relayed to the key users within each department.

6 Discussion

6.1 Project Results

Wien Energie GmbH is able to present an audit proof SAP ERP system which is applied globally within the company. Due to the project all roles are clear and easy to oversee. All identified duties are clearly separated according to the responsibilities of the receiving employee groups. A SoD approach has been implemented which follows the four-eyes principle as described in chapter 2.1. All related processes are executed by at least two employees, the approval process has to be delivered by a higher-level instance.

The project has defined and implemented all roles and the contained authorization objects. The roles follow a clearly defined structure which from now on sets the standard for all departments of Wien Energie GmbH. The IT Demand Management department is responsible for the creation of all new roles. The IT Demand Management department therefore uses existing roles as a template for the creation of new roles. What is more the department is handling the governance of the segregation of duties on the SAP ERP environment. The SAP GRC system continually examines the SAP ERP system for SoD conflicts so that possible exploits of the system can be promptly mitigated. For new employees as well as internal transfers the SoD principles eases the enrolment to their specific authorizations and duties.

The segregation of duties was implemented so fluidly that most employees would not notice big changes in their workflow. At the same time, a secure and state of the art authorization system has been created protecting the SAP ERP infrastructure was created. Key users of the system have been informed about the new principles and are now piloting the concept throughout Wien Energie GmbH.

The real impact of the project will show in the coming years when the practices have become the norm in the company. The secure authorization model with segregated duties will protect the SAP ERP system and the operations of Wien Energie GmbH in the future and allow more efficient and fluent operations in the company.

6.2 Findings

A key finding gained during the rollout of the project was in regard to the effort drivers. The project team assumed, that bigger departments (number of employees) would be the most complex to implement. It turned out that the size of the department had no impact on the complexity. The complexity is mainly driven by the intensity of system usage within a

department. Therefore, e.g. smaller departments which solely work with SAP created a much bigger effort for the project team than any other departments. This is due to when a department is more dependent and thus active on the system, more authorizations are required for them to successfully complete their work. As in the past, departments were individually managing their work and processes on the SAP environment authorizations were not restricted depending on the duties and position of the users within the organizational units, permissions accumulated. This led to the hazards described in chapter 2.1.1 becoming a serious threat to the processes at the affected departments. The roles and transactions within the departments accumulated to be harder to oversee and single users obtaining excess authority over the systems. This is to be anticipated when working on first controlled implementation of segregation of duties within a corporate SAP ERP environment. Interviews with key users and management are conducted after a preliminary analysis to gain an understanding of the origin and requirements of critical roles and transaction which cause conflicts.

6.3 Future development

With this project, Wien Energie GmbH has built an important foundation in regard to the implementation of the segregation of duties within their IT infrastructure. While the SAP ERP environment is a key component of the company the work must not stop here. The segregation of duties is a matter which is crucial to any system within a company and thus Wien Energie GmbH must continue and extend the work on implementing proper SoD within all their key IT infrastructures. This thesis aids future project teams as a basis on how to execute the segregation of duties in further projects. It is especially useful for the SoD on further SAP environments hosted at Wien Energie GmbH as the principles and structure are similar the one of SAP ERP.

Further, while the segregation of duties has been implemented into the SAP ERP system, the company must not rest as the changes must be upheld in the future. Many departments were self managing their work on the systems and thus may relapse to old practices. To combat this a change in company culture in the form of workshops and communication is required. The work must not stop there, and the practices must be reinforced not only through the IT department but through the leadership and management of all departments.

6.4 Conclusion

The segregation of duties in a corporate SAP ERP environment is a long and tedious process requiring patience, precision and a deep understanding of the systems and processes the changes are applied to. Proper authorizations are a crucial component of IT business infrastructures, which build the backbone of a company. User errors, exploitation and theft can lead to serious consequences for an organization. Thus, the access and abilities on a system need to be applied through the segregation of duties in order for proper handling of the system.

The segregation of duties ensures safety, efficiency and a clear overview of the authorizations, roles, and processes within an IT infrastructure. It protects the organization from dangers such as theft by employees, exploits benefitting business partners and errors caused by excess responsibilities combined with the lack of expertise. The most common approach is the four-eyes principle which segregates duties by requiring at least two people to complete a task. This has been successfully implemented through the project and creates the base for an extensive protection of the SAP system in the future.

In the case of creating an audit proof segregation of duties at Wien Energie GmbH hundreds of person hours were put in the analysis, planning and implementation of the SoD. The project team planned and implemented the segregation of duties successfully for all departments at Wien Energie GmbH ahead of the revised deadline. Each department was individually planned in order to allow continuous smooth operations and workflows on the SAP environment.

While the segregation of duties on the SAP ERP system of Wien Energie GmbH has been completed, the company must not stop there and enforce the created principles in the future. Further, the segregation of duties must be implemented into all IT infrastructures as the threads not only concern the SAP ERP environment.

6.5 Personal learnings and development

At the beginning of the project, when the author started working in the IT Demand Management team, he had no experience and knowledge on the processes and IT infrastructure of Wien Energie GmbH.

During his work on the project the author gained a proper understanding for corporate audit implications. Further he gained deep insights into a corporate SAP ERP environment and its administration processes. Additionally, due to his contribution on the planning and

implementation of the segregation of duties into the Wien Energie SAP ERP systems, he gained comprehensive knowledge on the matter of SoD and authorizations within large IT infrastructures. The training conducted at Wien Energie GmbH and the work on the thesis extended this knowledge.

It turned out to be more challenging to transcribe the daily work routines on the project into a written format on this thesis. There is a difference between theory and practice which makes the thesis even more valuable from a learning perspective as the theory gives more detailed explanation and multiple insights for certain elements of this project.

After the completion of the project and thesis the interest of the author for SAP ERP has grown significantly and he is now considering continuing his career in the field of SAP.

References

Association of International CPA's, 2020. Segregation of Duties. URL: https://www.aicpa.org/interestareas/informationtechnology/resources/value-strategy-through-segregation-of-duties.html. Accessed: 20 November 2020.

Banzer, A., 2017. COMPARISON OF SAP ROLE DESIGN CONCEPTS. URL: https://www.xiting.us/comparison-sap-role-design-concepts. Accessed: 26 October 2020.

Budhbhatti, C., 2014. BASIC UNDERSTANDING OF ROLES AND AUTHORIZATION. URL: https://blogs.sap.com/2014/10/09/basic-understanding-of-roles-and-authorization/. Accessed: 20 November 2020.

Dixon, S., 2018. EU Auditor Market Share: 2017 Audit Reports. URL: https://blog.auditanalytics.com/eu-auditor-market-share-2017-audit-reports/. Accessed: 20 November 2020.

European Commission, 2020. Auditing of companies' financial statements. URL: https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/auditing-companies-financial-statements_en. Accessed: 19 November 2020.

Gehrke, N., 2020. It's your (Segregation of) Duty! How well is your company performing when it comes to Segregation of Duties?. URL: https://www.zapliance.com/en/blog/segregation-of-duties-maturity-model. Accessed: 17 October 2020.

GRC Advisory, 2020. SAP GRC Access Control. URL: https://grcadvisory.com/en/products-services/sap-grc-products/sap-grc-access-control/. Accessed: 17 October 2020.

Kobelsky, K. W., 2014. A conceptual model for segregation of duties: Integrating theory and practice for manual and IT-supported processes. International Journal of Accounting Information Systems, 15, 4, pp. 304-322.

Kumar, S., 2020. SAP GRC Fire Fighter User Roles and Responsibilities. URL: https://expressgrc.com/sap-grc-fire-fighter-user-roles-and-responsibilities/. Accessed: 07 November 2020.

Oracle, 2020. What Is ERP?. URL: https://www.oracle.com/erp/what-is-erp/. Accessed: 20 November 2020.

Peatfield, H., 2019. How much does ERP cost?. URL: https://www.erpfocus.com/erp-cost-and-budget-guide.html. Accessed: 20 November 2020.

Perkins, B., 2020. What is ERP? Key features of top enterprise resource planning systems. URL: https://www.cio.com/article/2439502/what-is-erp-key-features-of-top-enterprise-resource-planning-systems.html. Accessed: 20 November 2020.

Petrascu, D., 2010. Internal Audit: Defining, Objectives, Functions And Stages. In: Studies in Business and Economics. Lucian Blaga University of Sibiu, Faculty of Economic Sciences. Sibiu. pp. 238-246.

Rouse, M., 2018. SAP ERP Central Component (SAP ECC). URL: https://www.computerweekly.com/de/definition/SAP-ERP-Central-Component-SAP-ECC. Accessed: 18 November 2020.

SAP PRESS, 2019. An Introduction to SAP GRC Access Control. URL: https://blog.sap-press.com/an-introduction-to-sap-grc-access-control. Accessed: 28 October 2020.

SAP SE, 2009. SAP ERP 6.0. URL: https://wiki.scn.sap.com/wiki/display/ESpackages/SAP+ERP+6.0. Accessed: 18 November 2020.

SAP SE, 2020. About SAP SE. URL: https://www.sap.com/corporate/en.html. Accessed: 8 November 2020.

SAP SE, 2020. Creating Composite Roles. URL: https://help.sap.com/viewer/ff4a624c6c551014b115b3f0358548b0/7.02.22/en-US/42271d24d86211d2961a0000e82de14a.html. Accessed: 26 October 2020.

SAP SE, 2020. Fourth-Quarter and Full-Year 2020. SAP SE. Walldorf. URL: https://www.sap.com/docs/download/investors/2019/sap-2019-q4-presentation.pdf. Accessed: 20 November 2020.

SAP SE, 2020. Organizational Unit. URL: https://help.sap.com/viewer/75721ed436354188aea60a1868a2a31c/6.00.31/en-US/4eeb68f410fd3990e10000000a42189b.html. Accessed: 26 October 2020.

SAP SE, 2020. SAP ERP. URL: https://www.sap.com/products/enterprise-management-erp.html. Accessed: 17 October 2020.

SAP SE, 2020. SAP ERP. URL: https://www.sap.com/finland/products/enterprise-management-erp.html. Accessed: 18 November 2020.

SAP SE, 2020. SAP History. URL: https://www.sap.com/corporate/en/company/history.html. Accessed: 20 November 2020.

SAP SE, 2020. What is SAP?. URL: https://news.sap.com/what-is-sap/. Accessed: 18 October 2020.

Sisk, A., 2018. 10 Steps of the Audit Process. URL: https://bizfluent.com/how-does-5296119-steps-audit-process.html. Accessed: 20 November 2020.

Software Path, 2020. What 3,000 ERP projects tell us about selecting ERP (2020 ERP report). URL: https://softwarepath.com/guides/erp-report. Accessed: 20 November 2020.

Szkoda, M. & Cieplik, K., 2020. Analysis of SoD conflicts in SAP ERP system logistics with the use of the SAP GRC application. In: MODERN SOLUTIONS IN PRODUCTION AND WAREHOUSING. s.l.:s.n., pp. 100-112.

The Economic Times, 2020. Definition of 'Authorization'. URL: https://economictimes.indiatimes.com/definition/authorization. Accessed: 20 November 2020.

Tuovila, A., 2020. Audit. URL: https://www.investopedia.com/terms/a/audit.asp. Accessed: 28 October 2020.

Tyndall, G., 2019. The Real Cost of an Enterprise Resource Planning System. URL: https://www.thebalancesmb.com/how-much-does-an-erp-system-cost-14132. Accessed: 20 November 2020.

United Nations Industrial Development Organization, 2020. What is the four-eyes principle?. URL: https://www.unido.org/overview/member-states/change-management/faq/what-four-eyes-principle. Accessed: 20 November 2020.

Wien Energie GmbH, 2020. Abfallverwertungsanlagen. URL: https://www.wienenergie.at/ueber-uns/unternehmen/energie-klimaschutz/energieerzeugung/abfallverwertungsanlagen/. Accessed: 3 November 2020.

Wien Energie GmbH, 2020. Corona: 53 Mitarbeiter gehen für euch in Isolation. URL: https://www.wienenergie.at/blog/corona-53-mitarbeiter-gehen-fuer-euch-in-isolation/. Accessed: 3 November 2020.

Wien Energie GmbH, 2020. Strom und Wärme für eine wachsende Stadt. URL: https://umwelterklaerung.wienenergie.at/de/2020/yXzjWVLC/energieversorgung/?page=1. Accessed: 3 November 2020.

Wien Energie GmbH, 2020. Unsere Energieerzeugung. URL: https://www.wienenergie.at/ueber-uns/unternehmen/energie-klimaschutz/energieerzeugung/. Accessed: 3 November 2020.

Wien Energie GmbH, 2020. Unternehmen. URL: https://www.wienenergie.at/ueber-uns/unternehmen/. Accessed: 17 October 2020.

Appendices

Appendix 1. Project-Contract/Commission (German)

Available upon request

Appendix 2. Wien Energie SoD analysis and planning training manual (German)

Available upon request