Universidad Carlos III de Madrid

www.uc3m.es

Double Major in Computer Science Engineering

and Business Administration

2015-2016

Bachelor Thesis

"Fraud Prevention through Segregation of Duties: Authorization model in SAP GRC Access Control"

Sandra Morillejo González

Thesis Supervisors:

Lluís Santamaría Sánchez

Jose María Sierra Cámara

Madrid 06/2016

ABSTRACT

The occurrence of cases motivated by fraud is becoming more prevalent in companies with weak internal control policies and security vulnerabilities. On one hand, internal fraud is usually carried out by top management or accounting positions which have higher privileges, and thus, more capabilities in the system to commit fraud. On the other hand, external fraud is managed by hackers who gain access to the internal information system through stealing employee credentials.

This project presents a solution to prevent fraud in companies. This proposal consists in controlling and managing user's authorizations through an Access Control principle: Segregation of Duties. Following this security philosophy, it is defined a role based architecture.

Furthermore, a detailed process on Segregation of Duties is carried out from a risk-based approach. Conflicts among critical tasks lead to significant risks in the system. Those risks become the core of the study. With an emphasis on risk management lifecycle, it is described every phase developed for achieving an implementation that complies with Segregation of Duties.

Based on the design proposed, it is depicted the methodology of a project, by using a tool that integrates and streamline risks, compliance, corporate governance and access control policies, which is SAP GRC Access Control.

Taking into consideration the security measures defined, costs of its implementation were calculated to be compared with the great losses occasioned by fraud and data breaches. The results showed that the percentage invested in security is almost imperceptible, ranging from 0.002% to 0.7% of the economic losses that fraud involves.

Finally, from the results presented and the methodology of the project performed, conclusions and recommendations are presented for enterprises to avoid fraud, through its detection and control.

TABLE OF CONTENTS

ABSTRACT 3
LIST OF FIGURES 8
LIST OF TABLES 9
1 INTRODUCTION 10
1.1 Introduction 10
1.2 Motivation 10
1.3 Objectives 11
1.4 Thesis Structure 12
2 BACKGROUND AND PRELIMINARY CONCEPTS 14
2.1 Enterprise Resource Planning (ERP) 14
2.1.1 Origin of ERP 14
2.1.2 Main features of a ERP system 15
2.1.3 Types of ERP 15
2.1.4 Reasons to acquire an ERP system 16
2.1.5 Advantages and disadvantages of ERP systems 17
2.2 SAP: Components and Structure 19
2.2.1 SAP R/3 Software 19
2.2.2 SAP Modules Structure 20
2.2.3 SAP HANA 22
2.3 SAP Security Architecture 25
2.3.1 SAP Security Settings 25
2.3.2 SAP Authorization Model Architecture 26
2.3.3 Architecture of SAP R/3 Authorization System 28
2.4 GRC: Governance, Risk Management and Compliance 36
2.4.1 Origin of GRC 36
2.4.2 GRC components 37
2.4.3 GRC Methodology 40
2.4.4 SAP GRC 40
3 ANALYSIS OF FRAUD: CAUSES AND PREVENTION 44

3.1 Fraud: types and causes 45
3.1.1 Individual vs Enterprise perspective 47
3.2 Accounting fraud & financial crimes 48
3.3 Cybercrime: Fraud & Security Breaches 55
3.3.1 Security Breaches Cases 55
3.3.2 Cost of Implementation of Security Measures to prevent breaches and fraud 60
4 FRAUD-PREVENTION STRATEGIES 67
4.1 Applicable Regulations 67
4.1.1 COSO: Internal Control Objectives, Components and Levels 67
4.1.2 Fraud Scandals' Legacy: Sarbanes-Oxley Act 68
4.1.3 Regulation for Internal Control and Corporate Governance Systems 70
4.2 Segregation of Duties 72
4.2.1 Segregation of Duties Model 73
5 SOD PROCESS FROM A RISK-BASED APPROACH 75
5.2 Risk Identification 77
5.2.1 Functional Matrix Definition 78
5.2.2 Technical Matrix Definition 79
5.3 Risks Analysis & Assessment 82
5.4 Action Plan 83
5.4.1 Stakeholders in decision-making 84
5.4.2 Mitigating Matrix Definition 84
5.5 Implementing Solutions 86
5.6 Measure, control and monitor risks 88
6 METHODOLOGY OF A SOD PROJECT USING SAP GRC ACCESS CONTROL 89
6.1.1 Overview of the most critical transactions and tables in SAP 91
6.2 Analysis of SoD 93
6.2.1 Identification of Critical Processes and Sensitive Transactions 93
6.2.2 Identification of critical authorization objects 94
6.2.3 Identification of Enterprise Structural Elements 95
6.2.4 Identification of Transactions for the Functional Matrix Definition 95

6.2.5 Risk monitoring and remediation using SAP AMR 96
6.3 Design 98
6.3.1 Critical Activities: Read-only access vs Read-write access privileges for the Authorization System Model 98
6.3.2 RBAC – Building a Role Based Access Control Architecture 98
6.3.3 Compliant Business Roles & SoD through SAP BRM 101
6.4 Implementation 103
6.5 Testing 103
6.5.1 SAP Deployment Environment 103
6.5.2 Security Analysis in the Quality Environment 105
6.5.3 User Access Management: ARM 106
6.6 Maintenance 107
6.6.1 Privileged access for critical tasks: SAP EAM 107
7 PLANNING AND COSTS 109
7.1 Project Planning 109
7.1.1 Monitoring Reports 110
7.2 Project Costs 113
7.2.1 Personnel cost 113
7.2.2 Hardware cost 113
7.2.3 Software cost 114
7.2.4 Other costs 115
7.2.5 Total costs 115
8 CONCLUSIONS 116
8.1 Recommendations and future development 119
9 Executive Summary 121
10 Appendix A: Additional SAP Security Configuration 124
11 Appendix B: Analysis of authorization objects for SAP CO module 129
11.1 SAP Controlling (CO) 129
11.1.1 Standard flow of the Controlling Business Processes 130
11.1.2 Authorization Objects Required 131
12 Appendix C: Solutions for Users' Access Denial 144

12.1.1 Solution to access: SU53 144
12.1.2 Solution to access: ST01 145

LIST OF FIGURES

Figure 1: *SAP R/3 Modules Structure. Adapted from (Lingard UK) and (The SAP Expert Base , 2000)___ 20*
Figure 2: *Submodules of SAP Modules FI, CO, HR, MM and SD. Source: Own elaboration.___ 21*
Figure 3: *OLTP vs OLAP systems (DataWarehouse4u, 2010) ___ 23*
Figure 4: *Breakthrough Data & Application Processing (SAP, 2014)___ 23*
Figure 5: *SAP HANA Platform - More than just a database (SAP, 2014) ___ 24*
Figure 6: *SAP HANA On premise Deployment (SAP, 2014)___ 24*
Figure 7: *SAP HANA Hybrid Deployment (SAP, 2014)___ 24*
Figure 8: *SAP HANA Cloud Deployment (SAP, 2014) ___ 24*
Figure 9: *SAP Authorizations Structure. Source: Own elaboration. ___ 27*
Figure 10: *SAP R/3 Authorization System. Source: Own elaboration. ___ 28*
Figure 11: *Identification of Authorization Objects in PFCG transaction in a Role Configuration. Source: Own elaboration. ___ 32*
Figure 12: *Authorization objects checked for transaction FPE3S, in transaction SU24 (SAP Security Analyst, 2014) ___ 33*
Figure 13: *Authorization field (TCD) in role ZS_DISPLAY_ALL_BASIS. Adapted from: (Consultoría SAP, 2016) ___ 34*
Figure 14: *Authorization values in role ZS_DISPLAY_ALL_BASIS. Adapted from: (Consultoría SAP, 2016) 35*
Figure 15: *GRC Structure (Deloitte, 2014)___ 37*
Figure 16: *Current State of GRC in some organizations (SAP GRC, 2007) ___ 39*
Figure 17: *Future State of GRC: organized, streamlined and efficient processes (SAP GRC, 2007) _____ 39*
Figure 18: *Integration of Business Areas involved in GRC along with SAP GRC tools for management. Source: Own elaboration. ___ 41*
Figure 19: *SAP GRC Access Control functionalities. Source: Own elaboration. ___ 43*
Figure 20: *The Fraud Triangle (Knop, 2016) ___ 45*
Figure 21: *The Fraud Diamond (BDO Consulting (BDOC), 2010) ___ 46*
Figure 22: *Combination of The Fraud Triangle and The Fraud Diamond: The New Fraud Triangle Model. Adapted from (Wells, Fraud Triangle, 2005) and (Lormel, 2012). ___ 46*
Figure 23: *Risk Management Lifecycle. Source: Own elaboration. ___ 75*
Figure 24: *Risk Identification Process. Source: Own elaboration. ___ 77*
Figure 25: *Legend of colors of a functional matrix. Source: Own elaboration. _____* ***¡Error! Marcador no definido.***
Figure 26: *Transaction FB01 documented (System, Authorization Object, values). Source: Own elaboration. ___ 81*
Figure 27: *Trace ST01 of transaction FB01 in SAP. Source: Own elaboration. ___ 81*
Figure 28: *SoD Project Phases where different actors are involved using SAP GRC Access Control tools. Source: Own elaboration. ___ 90*
Figure 29*: Corporate Governance: Risk and Compliance Integration. Source: Own elaboration. _____ 97*
Figure 30: *Flow of data across different environments. Source: Own elaboration. ___ 105*
Figure 31: *Monitoring Report on 15/04/2016. Source: Own elaboration. ___ 111*
Figure 32: *Monitoring Report on 15/05/2016. Source: Own elaboration. ___ 111*
Figure 33: *Monitoring Report on 15/06/2016. Source: Own elaboration. ___ 112*
Figure 34: *Burndown chart: Progress on Monitoring Reports ___ 113*
Figure 35: *Controlling Structure (Garmendia, 2012) ___ 130*

LIST OF TABLES

***Table 1**: Most used values in the activity field, ACTVT .Source: Own elaboration 34*
***Table 2**: Analysis of Cases about Accounting Fraud & Financial Cybercrime: Companies' Weaknesses, Originators of Fraud, Causes for committing it, Fraud Strategy, Economic Losses and Year of Occurrence. Source: Own elaboration. 49*
***Table 3**: Analysis of Cases about Cybercrime & Security breaches: Companies' Weaknesses, Originators of Fraud, Leak method, Fraud Strategy, Economic / Data Losses and Year of Occurrence. Source: Own elaboration. 56*
***Table 4**: Analysis of failures committed and security solutions that could have prevented them from occurring. Source: Own Elaboration. 62*
***Table 5**: Number of transactions executed yearly by users from the enterprises affected. Source: Own elaboration. 63*
***Table 6**: Security Software Solutions for the enterprises affected by security breaches. Source: Own elaboration. 64*
***Table 7**: Personnel costs for a SoD project. Source: Own elaboration. 64*
***Table 8**: Total Costs of Security Measures proposed. Source: Own elaboration. 65*
***Table 9**: Proportion of the cost of security measures against losses caused by security breaches. Source: Own elaboration. 66*
***Table 10**: Example of a functional matrix. Source: Own elaboration. 78*
***Table 11**: Example of a Technical Matrix. Source: Own elaboration. 81*
***Table 12**: Example of a mitigating matrix. Source: Own elaboration. 85*
***Table 13**: Legend of colors of a mitigating matrix. Source: Own elaboration. 85*
***Table 14:** Example of Rule set funcperm tab (based on the Technical Matrix Definition). Source: Own elaboration. 87*
***Table 15**: List of T-codes (SAP transaction codes) which are critical in SAP security configuration in a SoD project. Source: Own elaboration. 92*
***Table 16**: List of tables which are critical in SAP security configuration in a SoD project. Source: Own elaboration. 92*
***Table 17:** Project Planning. Source: Own elaboration. 109*
***Table 18:** Total Costs in Project Planning. Source: Own elaboration. 115*

1 INTRODUCTION

1.1 Introduction

Fraud is an important issue since there are many companies whose information systems are being attacked. Two key problems are the lack of internal control policies and the capability of fraudsters (hackers or employees) to commit fraud.

Currently, there are many users in the system who have access to different tasks in the same business process or in different business processes which can lead to perform conflicting tasks in the system. In order to build access control policies and reduce fraudsters' capabilities of committing fraud, it is needed to understand the Segregation of Duties (SoD) concept. This concept relies on the fact that a single person should not be able to record, authorize and settle a transaction. This thesis investigates the potential use of a model based on Segregation of Duties as a solution to prevent fraud. A tool that is being used in this research is SAP GRC Access Control which allows to implement Access Control as a security mechanism to analyze and identify risks, evaluate them, process and automatize rules for risk controlling, and monitoring of risks, among others.

1.2 Motivation

Notable fraud accounting scandals as well as significant data security breaches have represented the starting point of this study. Nowadays, almost every enterprise has suffered fraud once, or even several times. Moreover, its appearance and occurrence is expected to increase significantly in the foreseeable future.

By using complex hacking techniques, or using simple social engineering, intruders can 'easily' compromise the information systems of an enterprise. Security holes and weak internal control policies can determine the perfect scenario for fraudsters and hackers.

Analyzing the types of fraud and its causes, as well as the failures that many enterprises present in terms of control, security and policies create the basis for identifying the weaknesses of the company.

The motivation of this thesis is to analyze the solutions to prevent fraud and design a methodology which could be developed in a project form in companies.

1.3 Objectives

The impact that fraud causes in corporations is extremely high, nevertheless the risk of fraud is not generally well managed and valued by companies. Enterprises can suddenly lose significantly their brand's reputation and consumer trust due to internal accounting fraud or hacking attacks. That's why it is relevant to study Internal Control measures to prevent it, and provide a process where fraud risks can be mitigated and controlled.

The objectives defined to achieve through this research are the following:

Fraud prevention through Internal Control & ERPs

- Recognize main failures of companies that have been affected by fraud issues
- Comprehend the reasons that led hackers and fraudsters to commit fraud
- Identify measures to prevent fraud by companies
- Analyze internal control policies and regulation that support these measures
- Acknowledge the benefits of ERPs to identify business processes

Fraud prevention through Segregation of Duties in a security architecture

- Define a security architecture that supports a Segregation of Duties model
- Determine the extent of Segregation of Duties as a security tool to manage access control in companies
- Identify risks through Segregation of Duties and find out a process that describes the evolution and management of risks

Fraud prevention through a project based on Segregation of Duties & GRC

- Represent and determine the phases of a project based on Segregation of Duties
- Analyze the concept of GRC (Governance, Risk Management and Compliance) as a methodology for a SoD project
- Analyze the workflow of a SoD process and cooperation techniques when managing a project where different teams of different types are involved, such as internal control, IT security and financial departments have to work together for achieving integrated results

Fraud prevention through a project deployed in an ERP such as SAP based on Segregation of Duties & GRC

- Use an ERP such as SAP to provide a project of implementation of Segregation of Duties and Access Control
- Analyze security levels and authorizations that will provide a well-configured Access Control model

1.4 Thesis Structure

The present project is structured in 12 sections. The first 6 sections comprise the analysis, design of a solution, adjustment to current policies and regulations and a project methodology based on the solution proposed. The section 7 defines the planning and costs, whereas the section 8 include conclusions resulted from the project. In addition, section 9 includes an executive summary of the whole project. Finally, sections 10, 11 and 12 determine Appendixes A, B and C of the project, respectively.

Section 2 describes the current State of the Art of the involved technologies. It starts with a detailed description of an ERP, its origin and main features, types and advantages and disadvantages of using ERPs. Then, follows with a review on SAP structure based on modules and a short advance of SAP HANA. The next preliminary concept is the SAP Security architecture based on roles, profiles, authorization objects, clients… All these basic security terms are explained in further detail to fully understand the concept about how transactions are contained in roles which are assigned to users. The last preliminary concept is GRC (Governance, Risk Management and Compliance) which describes the work paradigm where different teams and business areas collaborate in the same project to identify, mitigate risks and to comply with the applicable regulation, within a corporate governance scheme. The tool proposed for carrying out all the functionalities mentioned is SAP GRC Access Control, which is described along with its main tools.

In Section 3 a description of the main types and causes of fraud is provided, as well as a review of a selection of fraud and accounting cases where fraud is involved and cases with significant security data breaches. The analysis of these cases provides the main failures and firms' weaknesses that lead to fraud. These provide the key points to design a model that reinforce such weaknesses.

Section 4 is devoted to the study of strategies that can prevent fraud, such as current regulations for Internal Control and Corporate Governance, and security principles for access control as the Segregation of Duties (SoD) concept.

In Section 5, it is implemented a Segregation of Duties process from a risk-based approach. Based on the risk management lifecycle, the SoD process is described. In the risk identification phase, functional and technical matrixes are defined to search SoD conflicts, thus, risks within business processes. In the next phase, risks are assessed based on the materiality of risk and it is analyzed its impact and probability. Then, in the action plan stage, anti-fraud strategies are implemented, so mitigating controls are established. In the implementation phase, mitigating controls, critical transactions, risks and rules are defined and included in the SAP GRC AC tool to set them out and automatically generate them. The last step is to monitor and continue measuring risks which have not been mitigated. The security process to build SoD is adaptive and continuous over time.

Section 6 states the methodology of a project based on Segregation of Duties, using tools such as SAP GRC Access Control. The project structure was based on an analysis-design-implementation-testing-maintenance scheme. Throughout every project phase, there are different tasks involved. The earlier stages are focused on SoD tasks, business processes and risks, but the next steps determine the Role Based Access Control architecture. This determine compliant business roles, using SAP BRM. The implementation phase is when this architecture goes live and consultants or support members can start assigning new roles to users so they can access their day-to-day transactions. The testing stage is when this model is created, modified and tested before being transported to the Production environment. The last phase is maintenance, which determine the ability for users monitoring when accessing critical tasks in the system.

Section 7 describes the planning of the whole project and the total estimated cost related to the work developed throughout this project.

Finally, Chapter 8 contains the conclusions extracted from the work done in this project and the work that has been left for future studies on the topic. In addition, section 9 includes an executive summary of the whole project for a complete vision of the objectives, conclusions and the analysis and results performed.

At the end of this thesis, there have been collected some additional information about SAP security configuration, a complete analysis of the most critical authorization objects in the SAP CCO module, and some solutions for users' access denial. These form the Appendixes A, B and C, respectively.

2 BACKGROUND AND PRELIMINARY CONCEPTS

2.1 Enterprise Resource Planning (ERP)

In this era of competition and economic crisis, innovating and communicating are essential verbs in every strategic plan of a company that tries to strengthen its image and competitive advantage. The way of communicating has changed. Managing social networks and constant innovation are steps that are transforming companies. Firms are focused on finding new solutions to their business problems, under the motto *Renovate or Die*. Regarding how firms manage their business these days, it has nothing to do with how companies coordinated processes or motivated people at work last century.

Nowadays we do not understand a business without a computer nor a business without a computerized software to manage its information.

2.1.1 Origin of ERP

Enterprise Resource Planning (ERP) systems started in the 1960s. ERP was born from its predecessor, Manufacturing Resource Planning (MRP) which was designed as an organizational and scheduling tool for manufacturing firms. First ERP systems widened the original MRP functionality beyond manufacturing firms' internal use, and included customers and suppliers. Then, other industries realized the benefits of ERP systems and started transforming its information systems. (The Resource Group, 2015)

In the 1970s, hardware and first PCs gained ground, shifting consequently business processes. Companies such as Oracle, JD Edwards and SAP formed. (The Resource Group, 2015) IBM presented MRP II: a closed-loop business process system, a cyclic business strategy based on 4 steps: 1. strategizing, 2. planning, 3. monitoring/analyzing and 4. acting/adjusting. (Turban, Sharda, Delen, & King, 2010)

The 1990s became the new era for ERPs with the rapid growth of technology on both software and hardware. (The Resource Group, 2015) ERP software systems integrated business processes through every functional area. It became an extensive system to manage multiple aspects of business operations: human resource management, finance management, operations management, manufacturing…This major evolution in ERPs resulted in the end of many vendors, however, others gained that competitive advantage, such as Oracle and SAP that weathered the storm and became the largest ERP vendors' firms, satisfying ERP's continuous functional changes.

2.1.2 Main features of a ERP system

An ERP system aims to optimally manage the resources of a company. That is why businesses in industries ranging from manufacturing companies to catering use ERPs to their benefit. The truth is that any business can realize a real ROI from the use of an integrated Enterprise Resource Planning system. ERPs streamline administrative functions and processes of business, making for higher efficiency and productivity – and less chance of error.

Most business can benefit from ERP, since such systems bring real-time visibility, control, insight, adaptability, flexibility and scalability.

ERPs streamline administrative functions and business processes, making for higher efficiency and productivity. Precisely because of that, ERP can be used in a variety of industries such as non-profits, retail, manufactures, governmental agencies, financial, etc.

2.1.3 Types of ERP

An ERP must fit essentially the enterprise needs, either having specific ERP modules that fit our needs by using a *modular ERP,* or a *customized ERP* solution.

Customized ERP solutions are specifically created for a company. Development and implantation are more expensive and risky than a modular ERP, however the resultant application will be perfectly adapted to the business. The risk of this solution is that it will be designed by a specific technological consulting company, so the maintenance and any additional solution to the existing ERP will be highly tied to this company. In these cases, it will be necessary to require to the consulting company a complete comprehensive documentation of the design, implementation and maintenance of the ERP solution deployed, so other future consultants can understand and work in other parts of the system efficiently.

The modular ERP solution is the most used since it is cheaper and faster to implement. The enterprise can hire as many modules or packages as required, that is why it is called ERP modular, since the business can hire only the purchasing module, or financial accounting module, CRM (Customer Relationship Management) module, warehouse management module… These modules are standard, so any consulting company will be able to help us to implement it or maintain it. Every module costs differently and fits different business needs.

Depending on where our ERP solution storage is located, we can distinguish between on-premise and cloud based solutions.

On-premise software installations reside on a dedicated server which is located within the enterprise intranet and maintained by the organization's IT department. This type of hosting provides additional control and validation. The IT department is responsible for managing this server, in addition to additional specific controls and validations that the company can set up for further security.

The on-premise solutions are the most used since there are still many companies which do not feel comfortable with cloud hosting and prefer the security that an on-premise solution provides.

On the other hand, cloud hosting is suitable for companies that do not want to worry about acquiring, installing, monitoring, upgrading and maintaining any hardware; besides not having an IT department dedicated for these tasks.

Cloud hosting software installation reside on a third-party server. Every update, backup, monitoring and upgrade is handled by the third-party at no additional charge. In order to access this server, the company will require Internet connection.

Cloud solutions are becoming more popular because of a lower initial cost, faster deployment than on-premise solutions, upgrades are managed by the service provider, they require a smaller IT team and scaling up this solution becomes easier since it is based on a pay as you go model.

SMEs usually use cloud solutions that can be rented, or even source ERP systems like Open ERP, Odoo, ERPNext… since Cloud ERPs is a more affordable solution for smaller companies with simple needs and tight budget.

Others solutions for SMEs with a higher budget could be using SAP Business One, A3 ERP, SAGE X3, Microsoft Navision, Solmicro Expertis… which can cost from €40,000 to €80,000. In contrast, ERPs for large enterprises such as SAP, Oracle or Microsoft Dynamics cost €100,000 and above. All these solutions can be either cloud or on-premise installed.

2.1.4 Reasons to acquire an ERP system

Many companies already have installed ERP software in their systems. Every year, hundreds of businesses look for advice in order to find an ERP that can fit their business needs. Improving integration between multiple disparate systems and business processes is the main reason to acquire an ERP, as confirmed by 59% of ERP buyers, analyzed through a survey by Software Advice (Burnson, 2015). 45% of ERP buyers mentioned that the second reason was to improve their CRMs software.

When companies face problems and frustrations as the following means that they need an ERP system.

1. *The company owns many different software for different processes*. Since the information is separated into various front- and back-end systems, retrieving this data becomes an arduous, complex and slow task, as well as quite inaccurate.
2. *Access to this information is not easily traceable*, since there are data silos, isolated sets of outdated business information gathered together from multiple software systems. Data is not reliable and its availability is not precise.
3. *Business process are irregular and lacking consistency*. This results in inaccurate data and poor business governance practices.
4. *Slow back office processes*. Manual accounting tasks and financial reporting across systems and through numerous spreadsheets determine very slow processes and unproductive employees.
5. *IT management across multiple systems becomes a very complex and time-consuming process* which is very costly and critical for the company resources. Update patches are expensive and require effort for customizing different IT software implemented.
6. *The company is not able to grow with the existing resources*. Because of the lack of integration of all the systems, it is hard to track if an order has been shipped when sales, inventory and customer data are maintained in separate databases. This fact creates poor reputation to customers and the sales service offered decreases globally.

Other factor that can promote companies to acquire an ERP system is to grow revenues and profits and expand operations. When companies want to put in place a new backend software systems and new processes, ERPs system is the solution.

2.1.5 Advantages and disadvantages of ERP systems

An ERP software allows multiple advantages for companies and their employees. ERPs offer a complete and robust functionality, which is secured globally. Using an ERP will allow companies to increase their sales and increase their profitability.

The main benefits that using an ERP system provides are the following:

- *Long-term savings*. This is the biggest benefit that an ERP can offer. This solution manages our business, processes, our assets, our human resources and our customers, all in one that provides a more efficient management which leads to long-term savings.

- *Speed and safety in decision-making*. By having available data from different departments on a screen and a well-defined planning allows managers to take decisions more easily. By having the whole image of the company on an ERP system, it is easier to determine weak points in the structure of the company in order to favor the company's growth, and improve the decision making process.
- *Better quality in the customer relationship management*. An ERP allows us to respond to customers in a shorter time. The way the ERP links all information in one place gives companies a faster traceability, in case of troubles in any of the stages of the value chain. Using the CRM module gives a more efficient way to deal with customers, thus, responsiveness to customers improves and we can meet market demand more efficiently, adapting quickly and safely to any change that customers claim.
- *Standardized organization*. Using an ERP forces different departments of a company to work in a more standard and ordered way. It helps to define best practices throughout the company. In this way, business processes are analyzed, standardized, automated and streamlined, ensuring greater efficiency in management. Because of that, information is very accurate and well integrated offering more autonomy in management.
- *Employee productivity*. As all processes are optimized, the productivity of employees increases. Jobs are automated by deleting those processes which duplicate or provide redundant information. In addition, ERPs are easy to navigate and very intuitive, so they will facilitate the work of employees.
- *Security*. The company information needs to be protected from information thefts or unauthorized access. ERP solutions provide different levels of access or authorization. Information is centralized and automatically backed up to prevent any failure. Cloud solutions also replicate information in different places.

All the previous benefits that ERPs offer are advantages of acquiring ERP systems. Basically, they give us a complete vision of all the important processes across all departments following consistent and automatic workflows. This unified system makes reporting tasks very accurate and on real-time. For this, ERP provides a centralized database system on the backend which store and backup all the enterprise data. Because of that, ERP systems are very helpful for managing enterprise companies globally located.

However, there are disadvantages that must be also highlighted:

- *Cost of ERPs are too high*. Cost not only comprises the cost of the ERP Software itself but also the planning, customization, configuration, testing, implementation, maintenance…

- *ERP deployments take a long time*. Installation of ERPs take from 1 to 3 years to get completed and – more complex in decentralized organizations
- *User participation is necessary*. It is important to provide user training. Although the user interface may be simple and intuitive, it takes time to learn how to use it for the same (and additional) tasks to what employees were used perform in other different software systems.
- *Migration of data to the new ERP system.* In order to integrate ERP systems in a unique ERP system, it is necessary to spend time, money and resources to achieve a consistent and complete migration of data to the new system.
- *Indirect costs*. There may be additional costs related to the ERP implementation such as new IT infrastructure, upgrade of the WAN links…

2.2 SAP: Components and Structure

What is 'SAP'? 'SAP' is an acronym for 'Systeme, Anwendungen, Produkte der Dataenverar- beitung,' in German, meaning 'Systems, Applications, and Products in Data Processing.' Founded in 1972, SAP – with its headquarters in Walldorf, Germany – is the world's leading business software company, supporting more than 50% of the world's enterprises.

SAP ERP is an integrated system that provides enterprises with the tools to manage strategic planning, control objectives and analyze operations. The main SAP system functionalities are: integration of business processes, multifunctional (Sales, HR, Purchases…), modular (based on modules or packages), enterprise wide and on 'real time'.

2.2.1 SAP R/3 Software

SAP R/3 is the former name of the SAP ERP. Its current successor is SAP ERP Central Component (ECC).

SAP based the architecture of R/3 on a three-tier client/server structure:

1. **Presentation Layer**: The newest version of R/3 GUI is based on SAP NetWeaver. SAP NetWeaver is the main computing platform of SAP SE, and it is the foundation for many SAP applications. SAP Web Application Server (or WebAS) is the runtime environment for SAP Applications and Business Suite Solutions such as SRM, CRM, SCM and ERP. SAP Netweaver is a service-oriented application and an integration platform. It is built using ABAP programming language, but it also uses C, C++ and Java EE.

2. **Application Layer**: This layer is composed by one or more application servers and a message server. A SAP application server is a collection of executables which can interpret programs developed with ABAP/4 language (4th generation) and can manage the input and output of these programs. In the server side, all SAP applications are held and run.
3. **Database Layer:** This layer contains all the information stored from the enterprise that is required by the ERP. The database layer receives requests from the application server when an ABAP/4 program is running and needs certain information stored in the database.

SAP R/3 communications are encrypted using SAP cryptography library for Secure Network Communications and Secure Socket.

2.2.2 SAP Modules Structure

One of the principal reasons why SAP is so popular is that it is really flexible and almost any of their features are customizable.

The way to achieve this flexibility is to break SAP system into different modules like HR, Finance, MM and so on, which emulate business processes of a department or business unit. You can integrate one module with other or even integrate it with third party interfaces. These types of modules are called **'Functional Modules' –** they are solutions by line of business or 'department'.

The illustration below shows all functional SAP Modules which are offered by SAP R/3. One of them is a little bit different, **IS – Industry Solutions**. These solutions are based on industry-specific software and they are preconfigured for any client industry (aerospace, automotive, banking, construction, healthcare, life science, oil & gas, retail…).

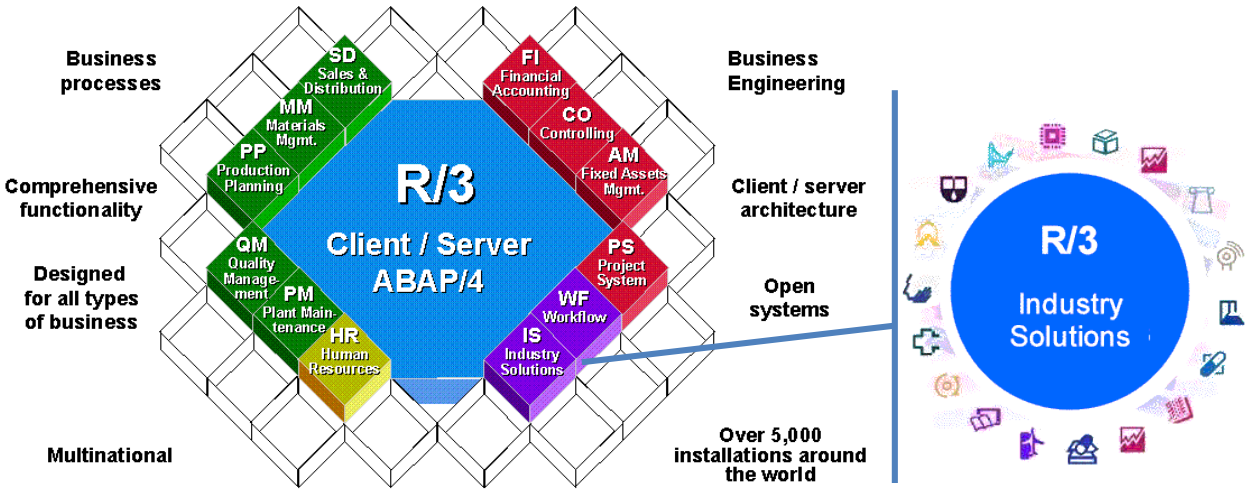


Figure 1: *SAP R/3 Modules Structure. Adapted from (Lingard UK) and (The SAP Expert Base , 2000)*

These functional modules are located in the Application Layer of SAP R/3 mentioned in the previous section.

Every SAP functional module contains submodules. The submodules below belong to some of the most important SAP modules: FI, CO, HR, MM and SD; the list increases frequently due to the fact that SAP releases submodules more customizable and functional.

Financial Accounting (SAP FI)	Controlling (SAP CO)	Human Resources (SAP HR)	Material Management (SAP MM)	Sales and Distribution (SAP SD)
• SAP General Ledger Accounting • SAP Accounts Payable • SAP Accounts Receivable • SAP Bank Accounting • Budgeting and Monitoring • Cash Management • SAP Asset Accounting • SAP Funds Management • SAP Treasury Management • SAP Special Purpose Ledger • Withholding Tax (TDS) • Travel Management	• SAP Cost Element Accounting • SAP Cost Center Accounting • SAP CO Internal Orders • SAP Profit Center Accounting • SAP Profitability Analysis	• Organizational Management • Personnel Administration • Recruitment • Payroll • Travel Management • Personnel Management • Time Management • Compensation Management • Training and Event Management • Wages • Personnel Development • Workforce Administration	• Purchasing • Inventory Management • Material Planning • Invoice Verification • Material Requirement Planning • Warehouse Management • Vendor Valuation	• Sales • Shipping and transportation • Billing or Invoice generation • Bills of Material • Sales Information System • Credit Control • Electronic Data Interchange

Figure 2: *Submodules of SAP Modules FI, CO, HR, MM and SD. Source: Own elaboration.*

On the other hand, there are "**Technical Modules**", based on innovation and functionality:

- Platform and Technology Solutions. These modules offer the basis to streamline complexities for real time responsiveness. These modules provide actions in a timely, trustful and innovative manner. Some of these solutions are Analytics Technology, IT Management, Security, Data Management…

- Solutions Spotlights. These are used to leverage business applications with the latest technology advancements. Some examples are Big Data, Cloud, SAP HANA Platform, SAP S/4HANA and Internet of Things.

Apart from SAP as an ERP, we can also highlight other product categories that it offers to help you run and optimize your software from SAP. Enterprise Management, Customer Relationship Management (CRM), Supplier Relationship Management (SRM) and Supply Chain Management (SCM) are some of these products.

SAP products oriented to small and medium size companies are SAP Business One and mySAP All-in-one.

2.2.3 SAP HANA

Due to its popularity and innovative architecture, the issue that concern us in this section is SAP HANA.

In-Memory technology is a new technology that substitutes the current Data base management systems technology.

SAP was pioneer in the introduction of this new technology in 2011 with their In-Memory platform SAP HANA.

The MIT technical database management academic team, recognized that In-Memory technology will replace the current Database Management Systems technology in presentation on august-24-2013 at MIT in Boston MA.

Database Vendors, like IBM, Oracle and Microsoft, are entering the market with new products IBM DB2-Blu, Oracle – In-Memory, in late 2013.

SAP HANA is a one in-memory atomic copy of data for transactions and analysis. Compared to the traditional databased approach, it eliminates redundant data copies, reducing unnecessary complexity and latency. Thus, there is less hardware to manage, so it accelerates through innovation and simplification.

In traditional systems, OLTP (Online Transaction Processing) provided source data to data warehouses, such as large number of master data transactions (INSERT, UPDATE, DELETE) that required an accelerated query processing, while keeping consistent data integrity in multi-access environments. On the other hand, OLAP (Online Transaction Processing) helped to analyze this information through data mining, analytics and decision making. This system requires lower workload of transactions, however it is more complex and involve aggregation structures and history data by using more indexes than OLTP.

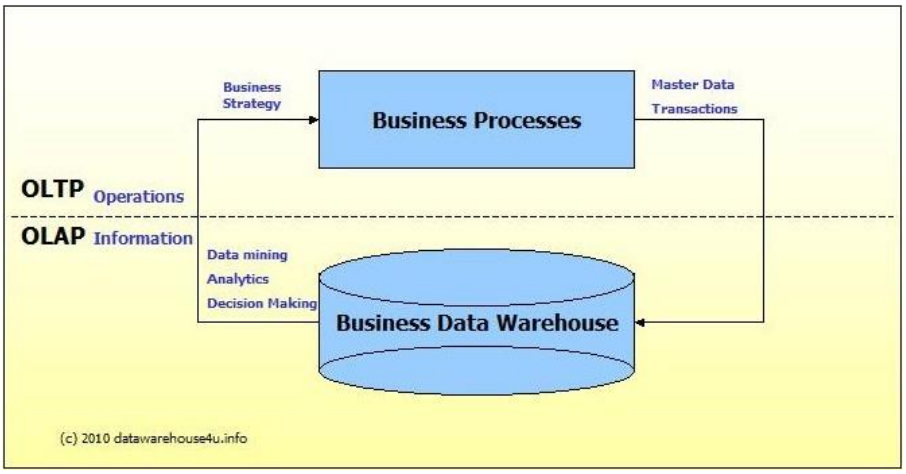


Figure 3: *OLTP vs OLAP systems* ***(DataWarehouse4u, 2010)***

SAP HANA permits OLTP (Online Transaction Processing) and OLAP (Online Analytical Processing) workloads on the same platform by storing data in high-speed memory, organizing it in columns and partitioning and distributing it among multiple servers.

This process delivers faster queries, avoiding in this way costly full-table scans and single column indexes. Compared to the previous image, it is evident how SAP HANA reduces its operational overhead and it leverages one infrastructure for analytical and text search in both OLAP and OLTP use cases.

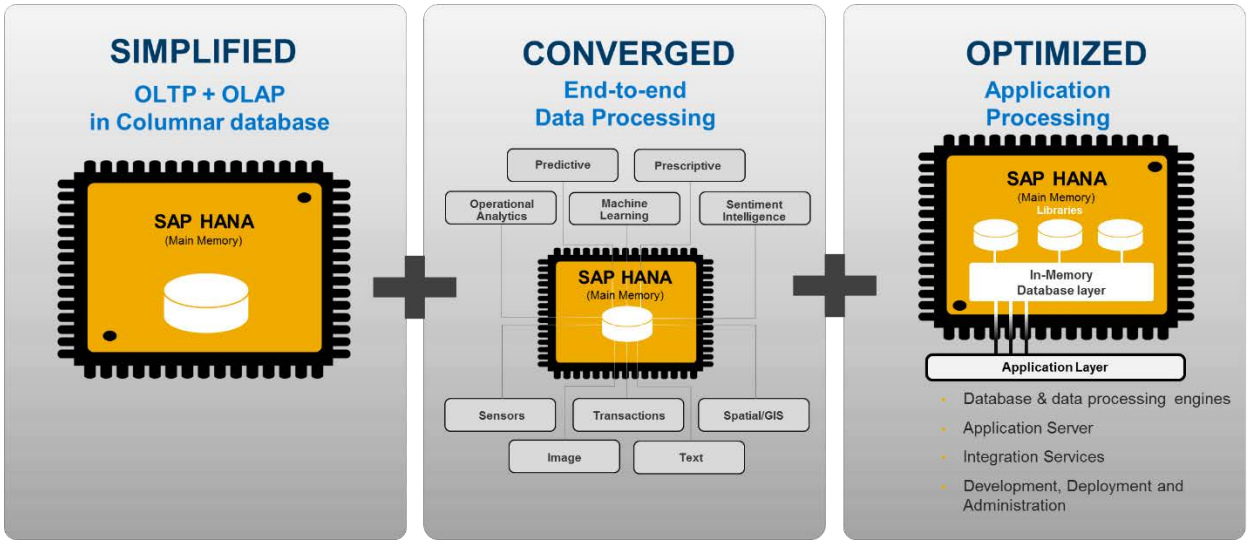


Figure 4: *Breakthrough Data & Application Processing* ***(SAP, 2014)***

SAP HANA platform converges Database, Data Processing and Application Platform capabilities. It also provides libraries for predictive, planning, text, spatial and business analytics allowing real-time business operations.

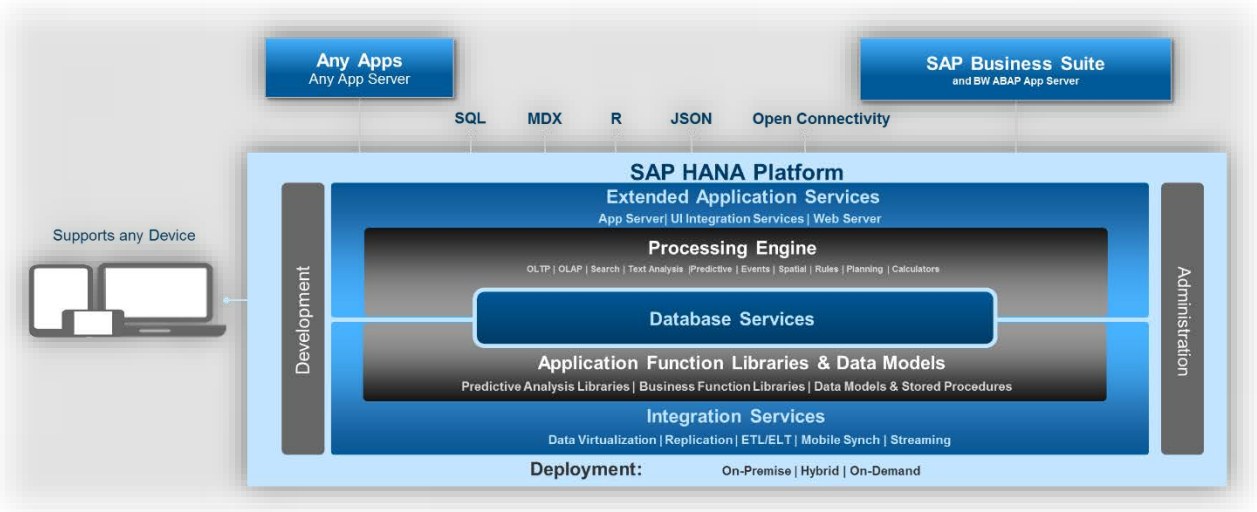


Figure 5: *SAP HANA Platform - More than just a database* ***(SAP, 2014)***

Moreover, SAP HANA offers three different deployment options which provide security, privacy and availability. Any of these options can be changed anytime:

1. **On premise** – Running all SAP Solutions on SAP HANA. The client can build or deploy own solutions on SAP HANA. These solutions are maintained all within the client's firewall.

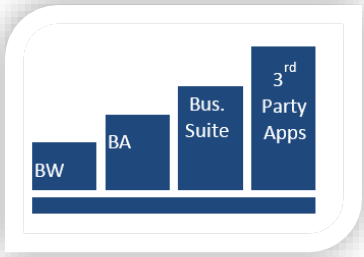


Figure 6: *SAP HANA On premise Deployment* ***(SAP, 2014)***

2. **Hybrid** – Leveraging SAP Cloud. Some solutions are migrated to the cloud, and you can also create or deploy your new SaaS apps in the cloud. In this way, the client can use cloud hosting and manage services deploying via SAP HANA Enterprise Cloud or using a public cloud.

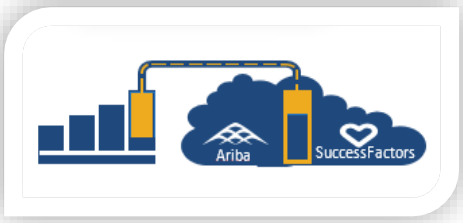


Figure 7: *SAP HANA Hybrid Deployment* ***(SAP, 2014)***

3. **Cloud** – Build, Run and Deploy all applications in the Cloud. This deployment option enables faster innovations and simplify the whole infrastructure. SAP HANA Enterprise Cloud provides the landscape to migrate client's applications or build new ones.

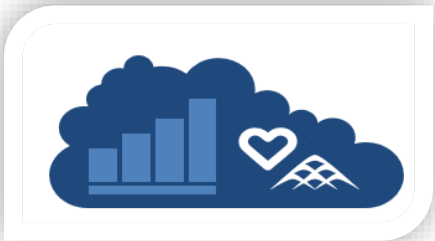


Figure 8: *SAP HANA Cloud Deployment* ***(SAP, 2014)***

2.3 SAP Security Architecture

Security in information systems involves protecting a company or organization's data assets. The practice that information systems security professionals carry out is based on testing, implementing, maintaining and repairing software and hardware used to protect information.

ISACA defines information security as measures that "ensure that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification or destruction (integrity) and non-access when required (availability)" (ISACA, 2012). In this way, a business or organization is secured to prevent crimes, espionage, sabotage or attacks.

In terms of SAP Security, SAP specialists are involved in installing and maintaining a secure SAP environment. However, it is not only their job, the entire IT department also has to contribute to secure SAP in the enterprise so that it is aligned with organizational policies.

2.3.1 SAP Security Settings

The security settings configured in SAP must comply with these principles:

1. Reducing internal fraud risks
2. Guaranteeing integrity, accuracy, confidentiality and availability of business data
3. Reducing unauthorized access risks to critical transactions
4. Regulatory compliance (SOX, penal code, LOPD…)
5. Control over the Production Environment and its transactions
6. Strengthening internal corporate governance
7. Compliance with the requirements directed by Internal and External Audit

2.3.1.1 Settings parameters for passwords

In SAP system, there must be configured different security parameters for access control, such as Standard SAP password controls. Such controls are security policies established in order to authenticate users in the system.

These are some parameters created in SAP user profiles that are helpful in order to control users' access. Some examples are:

- LOGIN/PASSWORD_EXPIRATION_TIME: Number of days after the expiration day when users can change their passwords. The default value is 0. The recommended value is 30-45 days.

- LOGIN/FAILS_TO_SESSION_END: Number of times a user can enter an incorrect password before logon attempts in the system are finished. The default value is 3. The range allowed is from 1 to 99. The recommended value is 3.
- LOGIN/MIN_PASSWORD_LNG: Minimum number of characters required for entering as a password. The default value is 3. The range of values is from 1 to 99. The recommended value is 3 characters.

The previous parameters and others are defined in the transaction RSPFPAR.

In addition to these parameters, there are other Standard SAP password controls: passwords cannot be PASS or SAP, the first character cannot be '?' or '!', password can only be changed at most once a day, users cannot reuse the last five passwords, and so on. Passwords defined by the client as illegal passwords can be entered into SAP table USR40.

2.3.1.2 Access Control Settings

Regarding to security settings related to access control, there must be configured a customized enterprise authorization model.

SAP security establishes a **RBAC** approach, which means a **role-based access control** system. Such policy restricts users access based on mechanisms around roles, profiles and privileges.

The client must define which are the business processes involved in every department to be able to conform roles, and thereby, generate profiles. These roles are assigned to users to they have access to certain functions, transactions, reports or menus in the system. These terms (roles, profiles, transactions…) will be explained in further detail in the following section.

The main purpose of these access control settings is achieving an authorization model where authorization objects, transactions, users and programs are defined correctly and reported appropriately. In this way, consultants can determine access control policies and roles according to the segregation of duties controls established.

2.3.2 SAP Authorization Model Architecture

Initially, a user has no access in SAP. When we create access in the system for a user, it is defined its UMR (User Master Records): basic information about the user such as name, password, user group… and authorizations that this user has in the system.

All this information is structured building 'blocks' that act as containers for other blocks of information. Technically, it is known as ABAP authorization model, which is built in SAP.

SAP provides authorization objects that allow users to define authorizations. These enable users to specify which actions they are allowed to execute in the SAP system. Authorizations that cover a set of tasks can be grouped together to form an authorization profile. Profiles are either created manually or automatically through the role generation. Roles describe functions that different people perform.

The primary rules defined by this RBAC model is:

- **Role assignment**: A user will be able to execute a transaction or a determined functionality in the system, thus, execute its permission if this subject has been assigned the role or profile for it.
- **Role authorization**: A role must be created in order to grant access to particular functionalities, thereby, users that are assigned this role will be authorized for it, and not any other action but what the role authorizes. Roles contain intrinsically profiles which include all the authorizations, however, users can be assigned also profiles without the necessity of assigning roles.
- **Permission authorization**: As mentioned in the rule above, users will be able to exercise a permission if that permissions is active previously in that role. Permissions, known as authorizations in SAP, contain the block of the authorizations and activities allowed by a role. If authorizations are not correctly set up in a role, users that are assigned that role, will not be able to execute it.

This round structure below represents how the architecture model is formed of a continuous grouping of authorization packages. The smallest package is the authorization object which is formed by authorization fields. The highest level is the Master Users' Records which keeps the authorizations for the user, such as roles and profiles

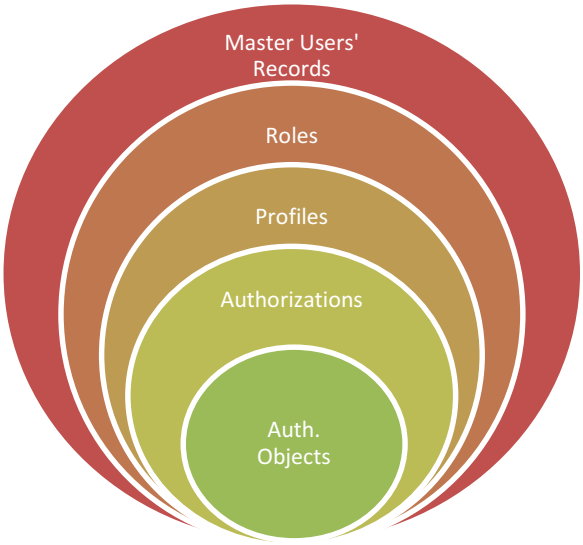


Figure 9: *SAP Authorizations Structure. Source: Own elaboration.*

2.3.3 Architecture of SAP R/3 Authorization System

The diagram below represents the SAP R/3 authorization architecture. It is represented using an UML Class Diagram.

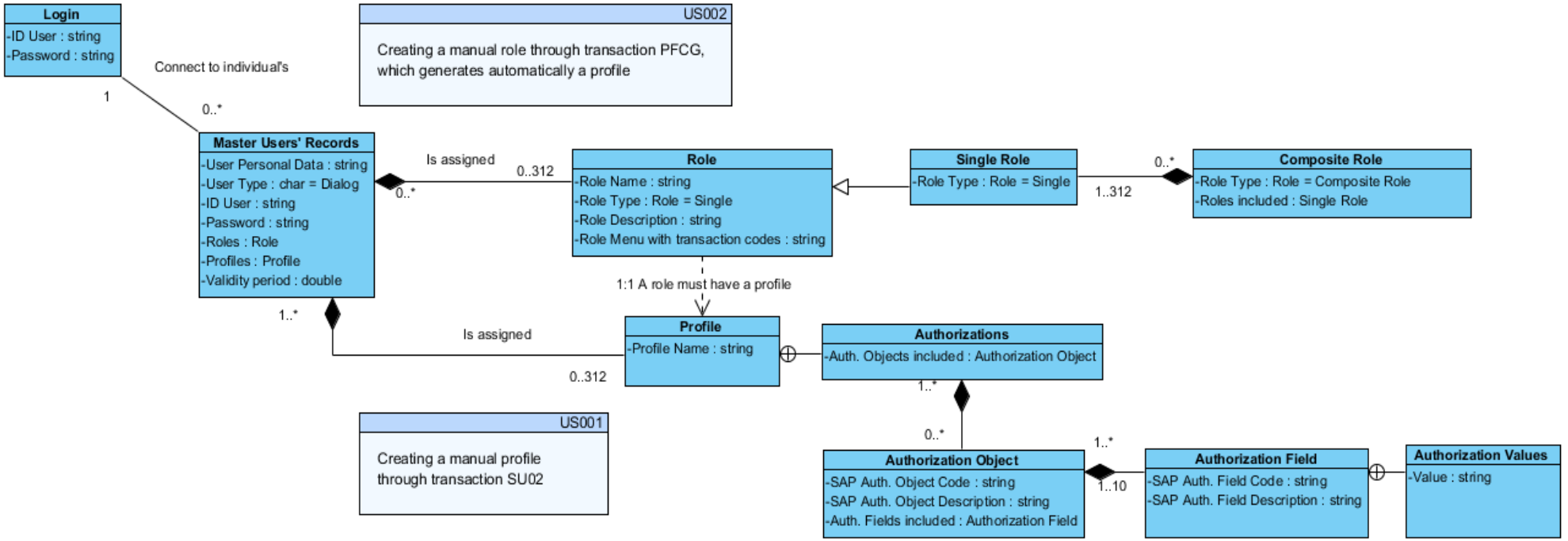


Figure 10: *SAP R/3 Authorization System. Source: Own elaboration.*

.

2.3.3.1 Master Users' Records

Master Users' Records define the accounts for which users can access to the system. This user information is accessed through transaction **SU01**.

Some fields that are determined are:

- User personal data, such as name, function, department, telephone, email…
- ID User
- Password
- User type: system, dialogue, communication, service, reference
- Default screen that the users sees at first when logging on the system
- Printers assigned by default to the user
- Users' groups
- Validity period
- Profiles
- Roles

See appendix A for more information about the configuration page of Master Users' Records.

As mentioned above, there are different user types that can be specified:

- **Dialog (A)**: Individual human users (end users from the business, including Internet users). Users are capable to connect through SAP GUI.
- **System (B)**: Background processing and communication users within a SAP system and between multiple systems, providing, therefore, internal and external RFC calls. Login from GUI is not allowed.
- **Communication (C):** Communication users for interfaces or external RFC calls among SAP systems. Login from GUI is not allowed.
- **Service (S):** Anonymous system access (such as for public Web services) that apply to a wide group of users, generally generic users that connect via an ITS (Internet Transaction Service).
- **Reference (L)**: Impersonal users, same as type S. Login from GUI is not allowed and they can be used to trespass their authorizations to the user that has it as reference.

2.3.3.2 Transaction

Transactions in SAP are similar to programs in ordinary computer languages. A transaction is a sequence of dialogue steps corporately consistent and logically connected. Performing a transaction makes the totality of each dialogue steps and update them. The graphical representation on the user screen and its logic process are called DYNPRO (DYNamic PROgram).

A transaction code or T Code is a four-digits short cut key to access a transaction. Transactions can be accessed either by its corresponding menu or by using the command field and entering the transaction code.

Custom transactions: Transactions that are created by the company for its interests should always start with Z or Y (the rest of letters are reserved by the system and for future SAP updates).

In order to execute a transaction, the user must have *at least* assigned within its master user record the S_TCODE authorization object. This object has the auth. field TCD, whose values determine the T Code of the transaction allowed to execute.

In addition to this object, there are other object validations that are required to execute a transaction, but S_TCODE is mandatory and essential for its operation.

The USOBT table shows the authorization objects associated with each transaction.

See appendix A for more information about how to enter a transaction in SAP by using its T-code.

2.3.3.3 Roles

Roles are a means to allow a user to access a transaction or to execute a particular function within a transaction.

A role consists of groups of transactions and activities that are created with a profile generator (PFCG). The role structure is a recipient that contains internally profiles (that include at the same time authorizations). Authorizations in SAP are privileges required to perform a specific function in SAP.

Thus, roles are assigned directly to users, so they are authorized to execute functions in SAP.

There are three different type of roles:

- **Single role**: an independent role
- **Derived role**: This role has a parent and differs only in organization levels. These roles are usually known as Organizational roles since they manage information related to the organization (centers, specific operations…). Transactions, menu and authorizations are only managed at the parent level.
- **Composite role**: It is a container that can include one or more Single or Derived roles.

See Appendix A in order to configure a single role in SAP with transactions associated and the process of assigning the role to a specific user (from transaction PFCG).

The AGR_USERS table displays the roles that are assigned to users in SAP.

Composite role consists of single roles. It eases user administration, so users can be assigned composite roles, and they are automatically assigned the associated single roles that compose the composite role. A composite role does not contain authorization data in itself, but the single roles which includes the authorizations needed.

See Appendix A to learn how to create a composite roles based on single roles.

The AGR_AGRS table displays the singles roles that are included in composite roles.

2.3.3.4 Profile

Profile is the core of the authorizations. A profile is basically a group of several authorizations, formed by authorization objects with certain values.

A profile is the minimum security unit that can be assigned to a user. The only way to assign authorizations to a user is to include them in a profile and assign that profile to users. Profiles can be assigned to users through roles or directly to the master users' records.

There are two ways of creating profiles:

- Using transaction SU03 (manually)
- Using transaction PFCG (automatically)

See Appendix A for configuring a manual profile by using transaction SU03.

Creating manually profiles does not have any advantage from creating it from the PFCG transaction. By using PFCG instead of SU03, it is faster due to the automatic profile process. In this way, profiles are linked directly to roles, so they are created based on functions (groups of activities). For this process it is not necessary a SAP administrator with expertise on authorization objects. However, authorization objects must be correctly maintained in the SU24 transaction. This transaction will be explained at the end of the following section, Authorization Object.

2.3.3.5 Authorization Object

An authorization object is the minimum security unit in SAP R/3. It identifies an element or an object that needs to be protected. Objects that belong to the same application

area such as Basis – Development Environment (BC_C) or Financial Accounting (FI) are grouped together.

Thus, authorization objects include organizational values such as organization, center, warehouse, cost centers, sales channel, etc.; and also the activities that can be performed on a task (create or register, change, display, delete, etc.).

The authorization system checks several conditions before allowing users to perform any task in the system. A multi-conditional check on an authorization object will allow users to create, view or delete information from a purchasing organization.

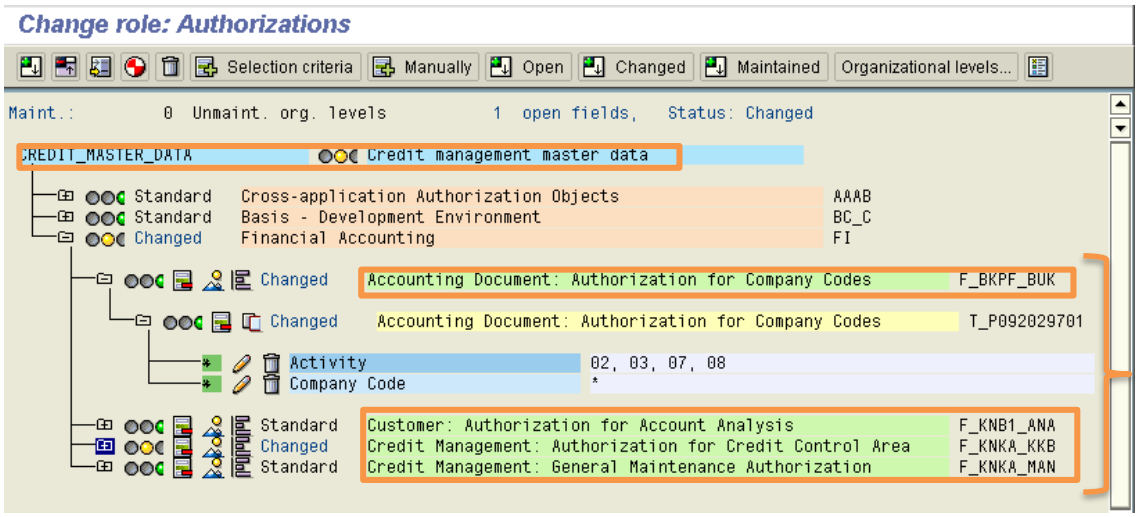


Figure 11: *Identification of Authorization Objects in PFCG transaction in a Role Configuration. Source: Own elaboration.*

The authorization object F_BKPF_BUK that is represented in the image above is in charge of controlling any modification (activity 02), reading (act. 03), activation (act. 07) or display of a changed document (08) that is done to the company code when accessing to an accounting document. Although this is a simple authorization object, there are authorization objects that allow you to define more complex authorizations.

SU24 is one of the most important SAP Security transaction codes. It is used **to maintain authorization objects** which are checked during the execution of a certain transaction.

On one hand, SAP predefined transactions have their own authorization objects already registered in this transaction, however, the enterprise can change its configuration in order to check the SAP standard authorization objects or not. In addition, the company can also add new authorization objects to be checked.

On the other hand, for each new transaction (designed by the own organization for business reasons), authorization objects must be documented in SU24, so these objects are checked by the system when you execute it.

In the transaction SU24, the objects that need to be checked to access this transaction are added in the following way:

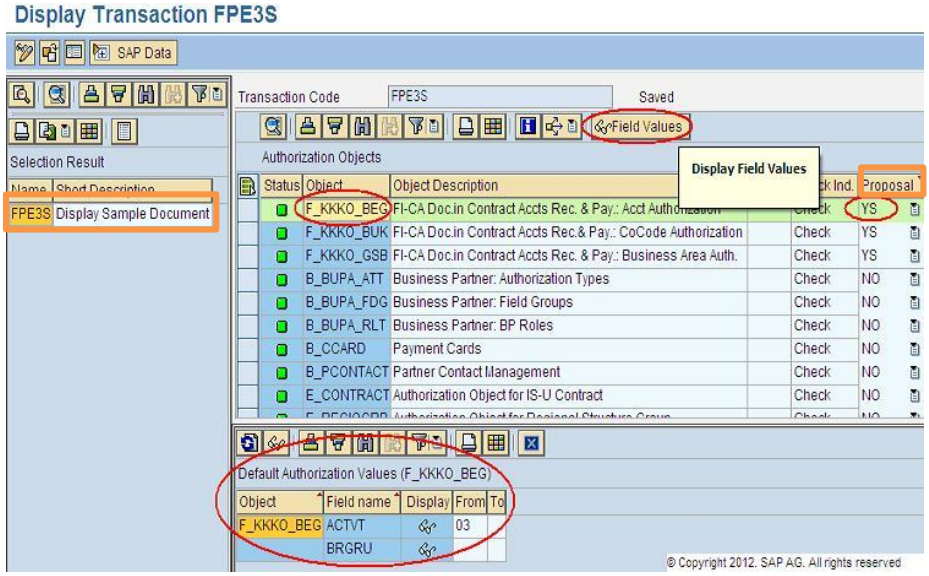


Figure 12: *Authorization objects checked for transaction FPE3S, in transaction SU24* ***(SAP Security Analyst, 2014)***

In the transaction SU24, we can display the authorization objects that are being checked for any transaction. In the example above, the transaction FPE3S has all these authorization objects, but the authorization objects that are checked by the system are those which are marked in the 6th column (Proposal) as 'YS' such as the authorization objects F_KKKO_BEG, F_KKKO_BUK or F_KKKO_GSB. Those which are marked as 'NO' are not checked by the system, so you do not need to have any specific role or profile with these objects to access to transaction FPE3S.

2.3.3.6 Authorization field:

An authorization field determines the system elements that need to be protected, by assigning to it an access value. Authorization fields may be referred to business information or security related configuration such as:

- User groups
- Company code
- Purchasing organization
- Development class

In the same authorization object, there can be maximum 10 authorization fields.

There is an authorization field which is included in most authorization objects that determine the activity permitted over a control such as company code, an accounting document type, an order type…

This activity field (ACTVT) has many possible entries. However, there have been selected in the table below the most used values.

ACTVT	Description
01	Create or generate
02	Change
03	Display
04	Print, edit messages
05	Lock
06	Delete
07	Activate, generate
08	Display change documents
09	Display prices
16	Execute

Table 1: *Most used values in the activity field, ACTVT .Source: Own elaboration*

The whole list of standard values of the activity field is in the TACT table. The relationship between activities and authorization objects is in the TACTZ table.

Authorization fields are part of the standard ABAP authority-check function that checks whether a user has certain values in an authorization object or not.

The TOBJ table contains what fields are associated with each authorization object, that is the way in which SAP knows which fields an authorization object contains.

When an object is assigned values to its fields, it is transformed into an **Authorization**.

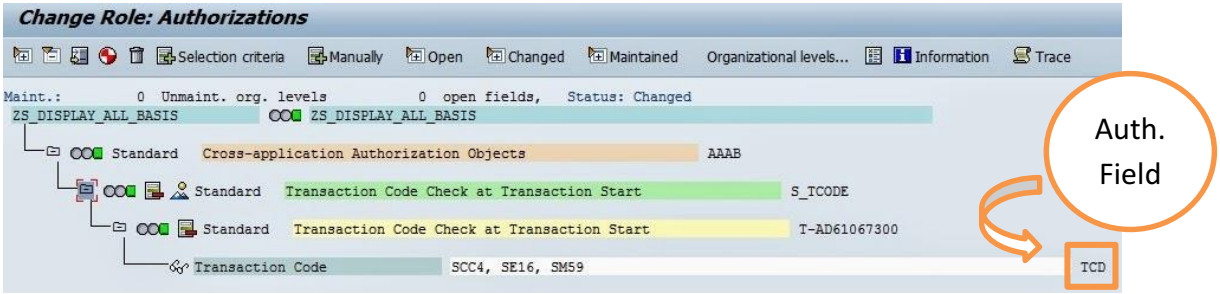


Figure 13: *Authorization field (TCD) in role ZS_DISPLAY_ALL_BASIS. Adapted from: (Consultoría SAP, 2016)*

2.3.3.7 Authorization value

Each authorization field has certain number of simple values. These values allow users perform specific actions in the system (in the image below, specific transactions).

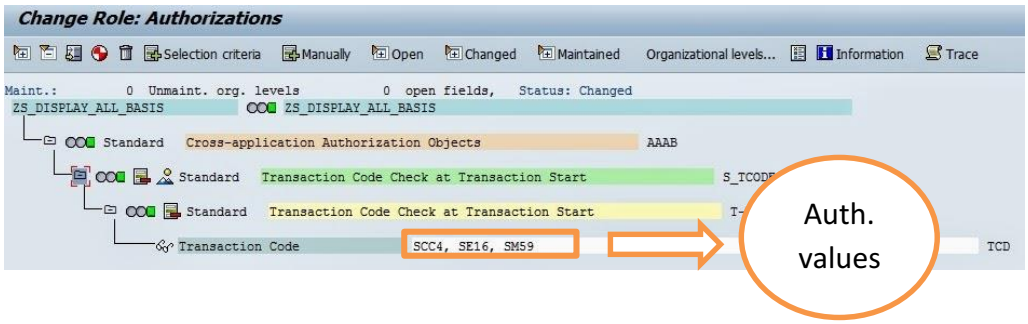


Figure 14: *Authorization values in role ZS_DISPLAY_ALL_BASIS. Adapted from: (Consultoría SAP, 2016)*

The authorization object TCD has the values SCC4, SE16 and SM59. The authorization object TCD defines the record of a transaction, the T Code. The first validation when accessing a transaction is checking the authorization object TCD of that specific transaction. In the image above, a user with the role ZS_DISPLAY_ALL_BASIS will have access to transactions SCC4 (Client Administration), SE16 (Data Browser – allows access to SAP Tables) and SM59 (RFC Destinations).

2.3.3.8 Client

In addition to the concepts addressed earlier such as Master Users' Records, Roles, Profiles, Transactions, Authorization Object, Authorization Field… there is another key concept in SAP that is relevant to analyze in the Security Settings: Clients.

A client is a subsystem or independent unit within a SAP system. The actions taken within each client are called transactions. These transactions are orders that call programs written in ABAP, which make internal transaction in the SAP system and query data from the database.

The default clients in the SAP system are 000, 001 and 066. The user SAP* and its password PASSS exists by default in these clients. It is important that during SAP implementation, all default user passwords in every client are changed.

From the perspective of security, clients should be closed and not allow modification to objects in the repository and to parametrization not dependent on the client.

The transactions SE06 and SCC4 must be restricted so they are not modifiable or customized. By using SCC5 consultants can clear a client.

2.3.3.9 Users

Managing users such as creating, modifying or deleting users, groups and roles is enabled using the UME (User Management Engine).

As an administrator, users and its authorizations for authentication can be controlled and simplified by collecting these users in groups. These groups are determined by their function in the company or the department they work for.

Roles is the best way to admin and control users' authorizations.

There are some transactions that provide user administration such as SV01. All transactions authorized to be performed by users are registered in the transaction SN01.

It is highly recommendable to establish security policies that force users to use secure passwords, using transaction SM30 -> USR40, through regular expressions, determining which are not valid passwords and through a dictionary with prohibited passwords.

2.4 GRC: Governance, Risk Management and Compliance

GRC, an acronym for *Governance, Risk Management and Compliance*, is the new term from Virsa systems.

2.4.1 Origin of GRC

Virsa Systems was a California-based compliance software maker. The Virsa tool was based upon a PwC preventative tool, known as SAFE, that controlled the grating and management of access within SAP. This was a tool used to check for SOX compliance in companies, and also very useful for finding the SODs in an enterprise.

On April 2006, SAP SE acquired Virsa Systems. This was part of a SAP strategic decision in order to create a new business unit to provide customer end-to-end solutions for GRC.

However, even before the GRC term was coined, activities and processes were monitored and managed attending to BAM (Business Activity Monitoring) and BPM (Business process management). These ideas were significantly important in the 2000s, so many solutions and tools gave birth to support companies BAM/BPM programs. Nevertheless, the implementation and maintenance of BAM/BPM projects were costly, and many companies abandoned them because of lack of results, integration issues, customization efforts… At the same time, external impositions forced companies to control their business and comply with the current regulations. This pressure created the need to implement better governance, more effective internal policies and accountability and consistent risk management.

Companies required specialized software to centralize governance, risk and compliance in order to establish risk and control frameworks; reporting their risks, controls and policies; deploying procedures to update risk exposures… These processes and systems came under the GRC umbrella term.

"Governance, Risk Management, and Compliance (GRC) are three pillars that work together for the purpose of assuring that an organization meets its objectives. (…) Governance is the combination of processes established and executed by the board of directors (BOD) that are reflected in the organization's structure and how it is managed and led toward achieving goals. Risk management is predicting and managing risks that could hinder the organization to achieve its objectives. Compliance with the company's policies and procedures, laws and regulations, strong and efficient governance is considered key to an organization's success." (Reding, et al., 2013)

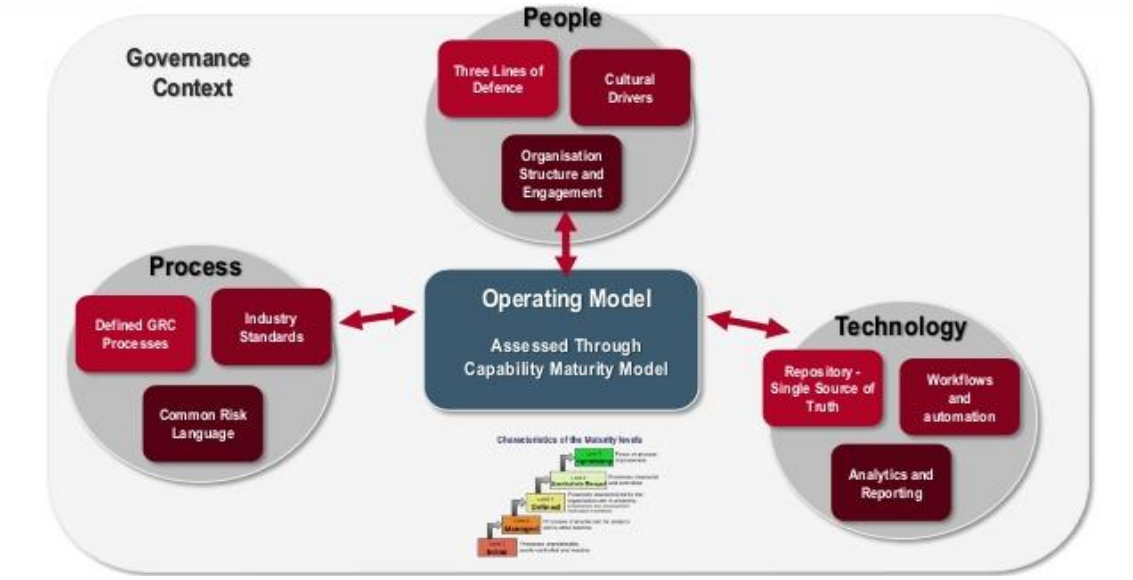


Figure 15: *GRC Structure* ***(Deloitte, 2014)***

GRC settles down different responsibilities in every business. In general, GRC means how governance, risk management and business' normative compliance integrate people, processes and technology.

2.4.2 GRC components

Governance describes how an organization is managed by top managers through information systems and management control structures that enable them an agile decision-making process guaranteeing the business strategy defined. Governance determines the internal company guidelines.

A corporate governance model is based on the enterprise characteristics. It addresses the differences between agent and principal. The agent problem is referred to the relationship between the business owners and the management thereof. The problem arises when the principal or shareholders delegate the agent (administration) the management of the enterprise in which the interests of one another are not always the same, resulting in asymmetric information.

The corporate governance model should establish the best system that encourages greater efficiency, safety and transparency based on the own business features and markets.

Risk management consists of a set of processes that allows management to identify, analyze and respond to risks that can adversely affect organization objectives. Risk management have to respond to risks through controlling, avoiding, accepting or transferring them to a third party. Risks involve many areas from technological risks to commercial or financial risks. Risk management considers internal and external guidelines that affect the company.

The enterprise must establish its risk strategies, taking into account the business impact of each of these risks.

In order to analyze efficiently risks, a threat and vulnerability matrix must be implemented, as well as risk analysis remediation to prevent possible risks. An action plan is the method used to respond to existent risks in the organization.

Governance of risk management aims the prevention of excessive risk management by taking into account organization's tendency to risk.

Compliance is the legal verification that risk management of the corporate governance is efficiently fulfilling external directives and regulatory guidelines, such as SOX, Basel II, Solvency III… Compliance means 'according to the requirements stated, thus, ruled by policy enforcement that apply to the organization such as laws, regulations, contracts, strategies and policies. The company must assess risks and potential costs that are involved when complying these requirements. For that, the company will prioritize and implement any corrective control measures deemed necessary.

A GRC program can be just focused on an individual area, or segregated into different individual areas to monitor. The most common areas are:

- Finance and audit GRC
- IT GRC management
- Enterprise risk management

In many enterprises GRC current state is very unorganized, complex and structured in a fragmented way. Business processes are not correctly integrated, so there are many vulnerabilities in the system.

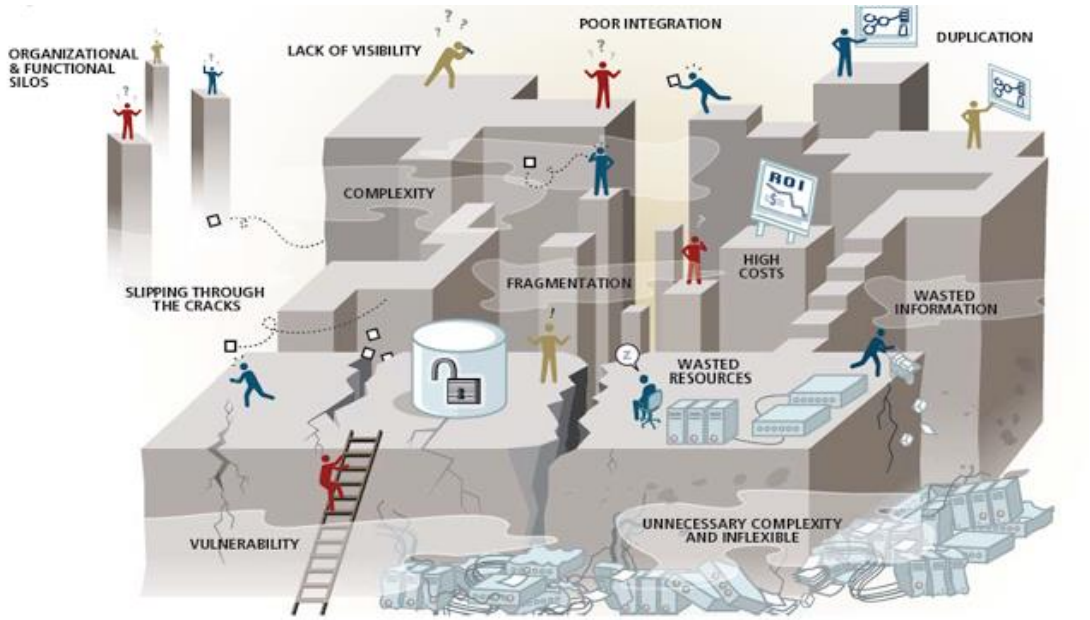


Figure 16: *Current State of GRC in some organizations* ***(SAP GRC, 2007)***

After deploying an automatized GRC solution that is focused on a risk-based approach, which rationalizes controls and redesigns procedures and it is supported by efficient technology tools, an enterprise will be able to standardize and streamline its processes through an integrated GRC system.

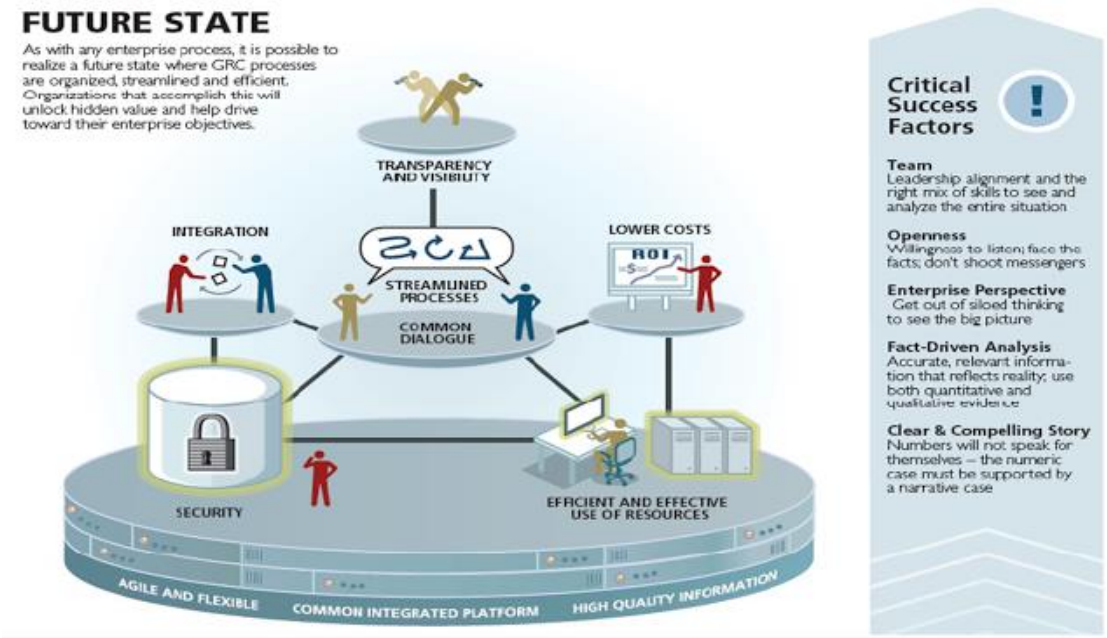


Figure 17: *Future State of GRC: organized, streamlined and efficient processes* ***(SAP GRC, 2007)***

After all being said, you may think GRC only affects big companies, or listed companies. However, GRC affects all companies, since corporate governance needs to be a critical concern independently of the size.

GRC is not only about documentation and reporting that must comply with government policies. GRC helps companies to build prerequisites for ensuring good governance and risk controls, beyond statutory compliance.

2.4.3 GRC Methodology

GRC approach is based on the implementation of methodologies that help Corporate Governance to:

1. Identify responsibilities of governance entities
2. Identify roles and responsibilities identified in the enterprise
3. Define risk in a common way throughout the organization
4. Build a common approach in the vision of the organization goals
5. Enabling responsibility for executive managers and business units
6. Design a consistent architecture and infrastructure in line with demand
7. Securing and monitoring this infrastructure
8. Ensure good management and scaling it with support groups of the organization

2.4.4 SAP GRC

The SAP GRC solution is a complete set of tools that ensure that risks throughout all business departments are identified, mitigated and monitored, as well as access control techniques that are offered for managing business roles and user provisioning. Furthermore, this application provides compliance with current regulation on internal control and audit reports on critical access tasks.

SAP GRC changes the work paradigm in the departments involved in internal audit, risk management, compliance and IT security.

SAP GRC enables an integrated solution for risk and control, it helps companies to manage risk events and compliance over the whole organization, business processes and IT applications.

The enterprise must face barriers such as legal normative, internal policies, external regulations and risk events, for example, if our operations are involved in unstable markets. Such events could prevent an organization to meet its objectives.

Enterprises' objectives include sales' growth, operational efficiency, brand reputation, customers' satisfaction... These objectives lead to different type of processes where diverse teams take part and control.

These teams could be bounded up in 3: **Risks management**, **Internal Control and Compliance**, and **IT security management**. Depending on the enterprise size or structure, these teams could expand to other departments or areas.

SAP GRC creates synergies among business areas, building a collaborative workplace for the mentioned teams. Together with the above three teams, **Internal Audit Management** must guarantee that all these control systems are working correctly.

GRC is similar to the ERP concept, since it also creates synergies among different business processes. In this case, GRC creates synergies between different business areas and departments. The aim of an ERP is to manage the business. In contrast, GRC's aim is to **control the business**.

SAP GRC is a single product that integrates all this business information that involve different areas. As it affects diverse departments and it is formed by different functionalities, it may seem that SAP GRC is composed by different modules, but it is a unique system and highly integrated, not only with SAP components but with other ERPs or applications.

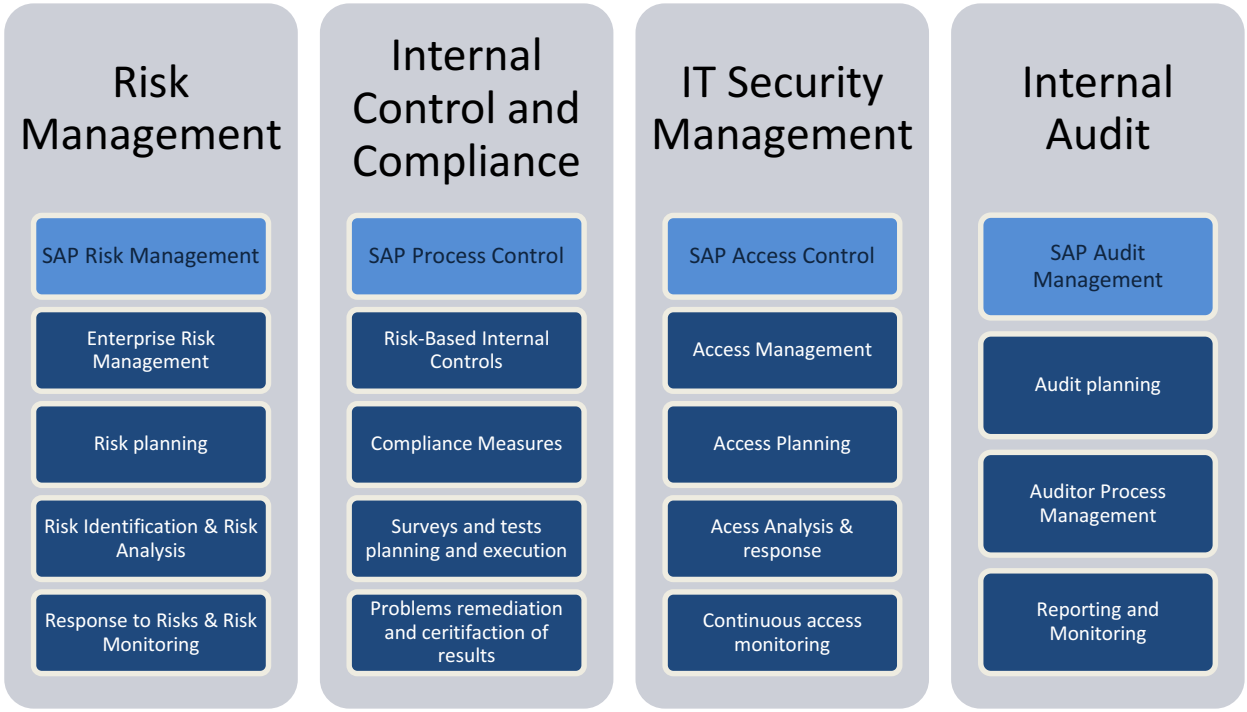


Figure 18: *Integration of Business Areas involved in GRC along with SAP GRC tools for management. Source: Own elaboration.*

SAP Risk management, SAP Process Control, SAP Access Control and SAP Audit Management are some of the tools provided by SAP GRC for implementing solutions to prevent fraud and manage risks in each of the enterprise areas involved in GRC.

In a quick overview of these SAP GRC tools, following the order of Figure 18:

1. SAP GRC Risk Management: supports both manual and automated risk identification and monitoring.
2. SAP GRC Process Control: ensures visibility and control by centralizing key controls of business processes that cross multiple systems.
3. SAP GRC Access Control: ensures adequate control of the segregation of duties
4. SAP GRC Audit Management: improves the way audit processes are carried out, through streamlining audit processes with intuitive documentation and increasing its efficiency with better planning and reporting methods.

However, **SAP GRC Access Control** is the most requested by companies since it allows to identify and analyze risks, manage user access, manage critical user access and user access provision. All-in-one. In addition, it is the most secure method for granting privileges in SAP.

2.4.4.1 SAP GRC Access Control

This tool enables enterprises to build **a security model based on roles** and authorizations that is designed upon the SoD model.

As we have described in the previous sections, segregation of duties helps to separate different functions that combining with each other would result in a situation where employees can commit fraud. In order to avoid it, SoD separate these sensitive tasks into different actions, that in security terms, are defined as roles. These roles can be configured to perform only the activities permitted in this process.

SAP GRC Access Control enables tools to build segregation of duties on the basis of a security architecture. As can be seen, this application is very powerful for the value it provides to firms: financial value, security value, business management, risk management value, internal control...

SAP GRC approach is focused on the development of business roles based on functions. This implementation is closely **linked to the HCM module** and the combination of both modules is greatly increasing since enterprises could **automatize privileges provisioning** when hiring or firing staff in the master entity personnel. The connection to HCM is made at the **functional role level** (based on business processes) which is related to job positions or HCM functions to achieve the automation model.

Every SAP function is related to business processes and standard functionalities within these, so the roles that are created for users **standardize enterprise processes** in a secure way. The role architecture that is built in SAP GRC has no compatibility problems, so it is complete and ready for assigning 'cleanly' these roles to users. Thus, it is a more sustainable and **maintainable model** over time.

The role model built eradicates any hybrid role or custom roles for specific users in the organization, so it becomes easier to manage and administer, plus risks of dependency functions are mitigated.

The basic tools that SAP GRC Access Control provides are:

1. Analyze and Manage Risk (AMR)
2. Emergency Access Management (EAM)
3. Business Role Management (BRM)
4. Access Request Management (ARM)
5. Risk terminator

All these tools are explained in further detail in the next section, where these tools are used for building a SoD project by using SAP GRC Access Control. Each of these SAP GRC AC submodules is intended for a determined phase of the project. However, they can be used simultaneously in different phases of the project if the firm needs them for specific reasons, such as reengineering roles or making changes in a test environment.

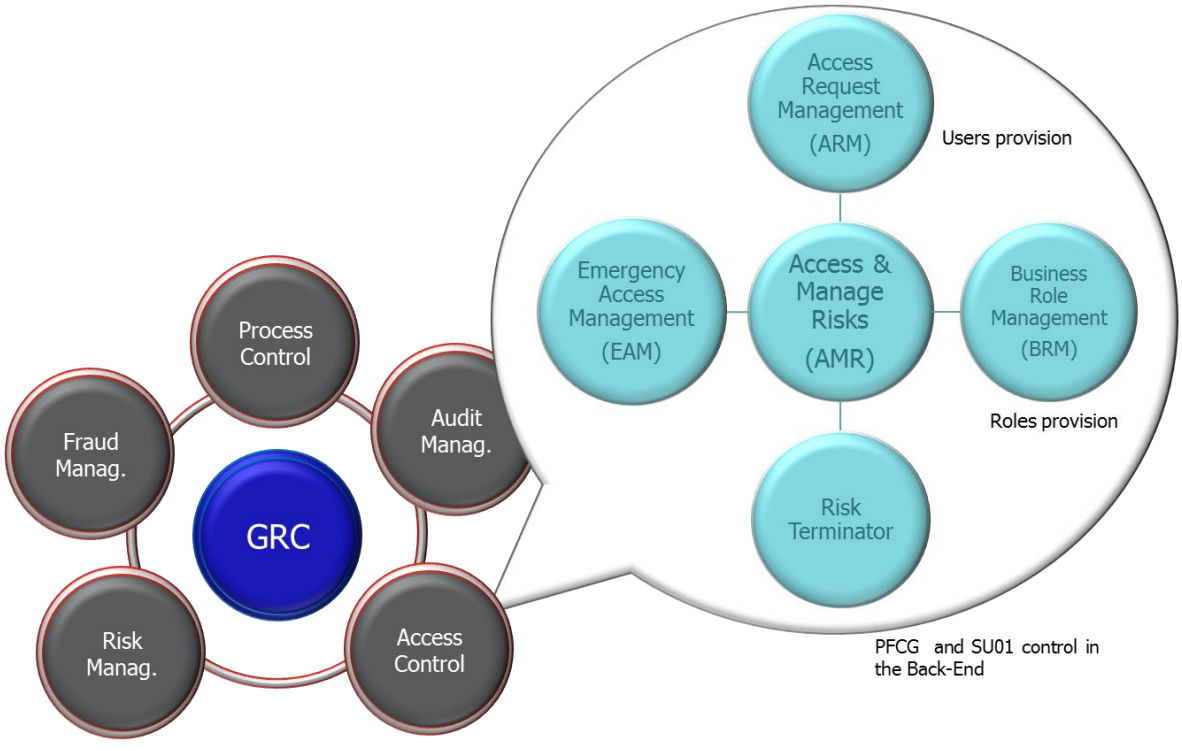


Figure 19: *SAP GRC Access Control functionalities. Source: Own elaboration.*

3 ANALYSIS OF FRAUD: CAUSES AND PREVENTION

One of the critical challenges faced by enterprises is the need to prevent fraud operations and manage them through appropriate security techniques in their information systems.

In a situation whereby inaccuracy of accounting entries occurs, there are two possible reasons for the discrepancy: error or fraud. On one hand, errors are unintentionally made and they often take place due to computer malfunction or human error (lack of knowledge, carelessness). On the other hand, fraud is intentionally committed and it is used to gain a dishonest advantage, which is usually financial, over another person.

Based on a research conducted between November 2014 and October 2015 on victims of cyber-crime in the UK, "70% of fraud is cyber enabled" (The City of London Police, 2016). Cyber-crime is defined as any crime that involves a computer and a network. One of the multiple activities that involve cyber-crime is **fraud and financial crimes**. Regarding to the study mentioned, the City of London Police is currently investigating an estimated £600 million in financial losses due to fraud and cyber-crime.

In this context, financial crimes can result from different ways:

- Altering data in an unauthorized way using unauthorized processes and data exploiting security holes (vulnerabilities in the enterprise's software system).
- Altering, destroying, suppressing or stealing output, usually to conceal unauthorized transactions.
- Altering or deleting stored data.

Other bank frauds are using computer systems including bank fraud, carding, identity theft, extortion and theft of classified information.

In section 3.2, there is an analysis of the four most significant financial fraud cases in the world: Enron, WorldCom, Bernie Madoff, Jérôme Kerviel and Pescanova.

Other cyber-crime activity is '**computer as a tool**' whose target is the individual and the tool is the computer, and it generally exploits human weaknesses or information security breaches. Some of these crimes are fraud and identity theft (using malware, hacking, phising…), information warfare, phising scams, spams and so on. This type of cyber-crime uses the computer as a tool and it generally exploits human weaknesses or information security breaches. The most outstanding IT fraud cases related to security breaches will be explained in section 3.3.

3.1 Fraud: types and causes

In the category of financial fraud, there are three different means through fraud is committed:

- Misappropriation of Assets: It occurs when an employee steals company assets. These can be physical assets: from office supplies to expensive items in inventory. Assets can also be monetary including cash or cash equivalents. These items are highly liquid and accessible. Poor internal controls provoke scenarios where employees can steal checks and cash them for themselves.

- Misrepresentation of Financial Statements, or also known as 'cooking the books'. It occurs when financial statements are intentionally misstated in order to make the financial position look better than it actually is. In order to get this appearance, reported revenues are increased and expenses are decreased. Misrepresenting balance sheet accounts can involve changing ratios such as the current or debt to equity ratios.

- Corruption: Dishonest behavior by those in positions of power, such as managers or government officials. Corruption cases include giving or accepting bribes, double dealing, under-the-table transactions, conflicts of interests, improper handling of relationships with custom agents, extortion, diverting funds, improper payments…

In order for fraud to occur, there must be given three conditions: **rationalization** by the person committing the fraud, **pressure** or **incentives** to commit the fraud and the **opportunity** to do so.

These three factors compose *'The Fraud Triangle'*, created in the 1950 by Dr. Donald Cressey, a criminologist whose research focused on fraudsters.

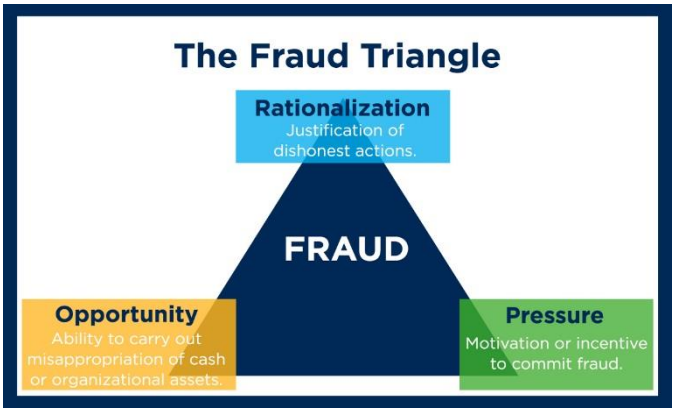


Figure 20: *The Fraud Triangle* ***(Knop, 2016)***

In 2004, Wolfe & Hermanson introduced the 'The Fraud Diamond' model, which added the fourth element: **Capability**.

This factor is related to personal traits, how a person plays a certain role in committing that fraud such as being confident, stress-dealing, authoritative and knowledgeable of the accounting systems and internal control weaknesses.

Figure 21: *The Fraud Diamond* ***(BDO Consulting (BDOC), 2010)***

In 2010, M. Kranacher proposed a model that mainly focused on one of these sides of the triangle: incentive or pressure, which she redefined as "Motivation of Fraud Perpetrators" (Dorminey, 2011). This factor was defined with the acronym **MICE** which stands for: Money, Ideology, Coercion and Ego. These type of motivators create that social pressure to commit fraudulent activities. However, as Dorminey argued, this model cannot solve the fraud problem since there are two sides that cannot be easily observed: *pressure* (or incentives or motivation), and *rationalization*, redefined as Personal Integrity in the Fraud Scale Model (Albrecht, 1984).

The combination of above models is reinterpreted as the **New Fraud Triangle Model** (Kassem & Highson, 2012) to better understand why fraud is committed as an extension to Cressey's fraud triangle model, including motivation, opportunity, integrity and fraudster's capabilities as shown in figure 11 below.

Figure 22: *Combination of The Fraud Triangle and The Fraud Diamond: The New Fraud Triangle Model. Adapted from* ***(Wells, Fraud Triangle, 2005)*** *and* ***(Lormel, 2012)****.*

3.1.1 Individual vs Enterprise perspective

This previous analysis of how fraud is committed and its motivators helps us to conclude that there are three sides of this triangle: motivation, fraudster's capabilities and rationalization, that depend largely on the *individual*. Individual *reasons* to commit fraud can be affected by others, but this fact is problematic to be controlled by the *enterprise*.

Fraudster's capabilities are applicable to the individual's skills such as the ability to deal with stress and pressure and confidence of not being detected. **Capability** is also affected by an authoritative position within the organization.

There are many **pressure** sources that can 'force' the individual to commit fraud. When speaking about pressure sources, we are referring to different **motivation** inflows:

- ✓ Personal pressure (gambling addiction; lack of personal discipline)
- ✓ Corporate or employment pressure (continuous compensation structure; frustration with work)
- ✓ External pressure (market expectations; social pressure).

This pressure can come from either financial or non-financial pressure. The enterprise measures may create pressure on the individual, consciously or not, in order to commit fraud.

Personal Integrity, as defined by the Fraud Scale, is "the personal code of ethical behavior each person adopts" (Albrecht, 1984). **Rationalization** is particularly applicable to financial reporting fraud, where sources of pressure are more observable such as analysts' forecasts, managements' earnings guidance and history of sales and earnings growth.

These pressures encourage individuals to adopt a fraudulent behavior that allows them, for example, to avoid loss of customers or a decline in sales which can hurt dramatically their image, ego or their sales incentives. This fraudulent financial behavior is present to some degree in all enterprises.

Nevertheless, **opportunity** is significantly different from the other triangle sides. This variable relies heavily on the enterprise opposition to fraud and the security measures it provides to prevent it. Enterprises must take a stand against fraud and endorse a healthy and safe work environment.

Fraudsters can commit fraud when they have a position of trust in the company and have knowledge about certain shortcomings in the internal control structure so they can compromise security access controls without being noticed.

3.2 Accounting fraud & financial crimes

In the last decade, many large cases of cybercrime have been noticeable due to accounting fraud. Some of these cases were carried out by a single individual, such as Bernard Madoff, Jérôme Kerviel and Manuel Fernández de Sousa. Usually, in these cases, justice is more severe and more comprehensive the market. However, when it comes to a company that leads the scam, reputation drops dramatically, along with its shares. The loss of trust in the company is immediate, severely damaging the firm, as happened with Enron and WorldCom, two of the largest US companies that staged the biggest financial scandals of the so-called globalization of capital markets. Simple operations marked by the ambition and greed, and not influenced by the financial crisis of 2008, which did affect Kerviel operations.

Before analyzing every case in further detail, in the following table, there is an overview of the cases being reported and some relevant features about them, such as:

1. Name of the company affected by fraud
2. Weaknesses of the company affected by fraud, which are company's failures that facilitated fraud to occur
3. Name of the originator of fraud specifying if it was committed by an individual or a collective (the company to itself or a third party group)
4. Intrinsic or extrinsic causes to individuals that incited them to commit fraud
5. Fraud strategy: Action plan to carry out fraudulent operations
6. Economic losses that resulted from fraud
7. Year of occurrence of the case described

Company affected	Company's weaknesses & failures	Originator of fraud: Individual or Collective	Cause for committing fraud	Fraud strategy	Economic losses[1]	Year
Enron	Individualism, undefined code of conduct, lack of access control, poor financial reporting	Arthur Andersen Consulting (Collective)	Huge incentives and bonuses if increased profits	- Destroying compromising documents in which billions in debt were hidden - Took advantage of accounting loopholes and special purpose entities	$ 63.4 billion losses	2001

[1] Figures of economic losses are represented in American billion dollars. American billion dollars are expressed as a thousand of million dollars. However, Spanish billion dollars are expressed as a million of million dollars. It is important not to confuse them since they are not equivalent.

WorldCom	Weak internal control for Top Management and Accounting Department	WorldCom Accounting Department, CEO & CFO (Collective)	$10 million in bonuses to CEO & CFO when not making profits	- Incorrect posting of operating costs as expenditure cost on the Balance Sheet - Loans & transfers granted not allowed by GAAP	$ 3.8 billion losses	2002
Madoff Investment Securities (BMIS)	Lack of internal control procedures	BMIS's CEO: Bernie Madoff (Individual)	High reputation in Wall Street, along with an authoritative position in BMIS	- Ponzi scheme: pyramidal fraud of investments - Gaining potential clients in exclusive clubs in the U.S.	$50 billion losses to customers	2008
Société Générale	Lack of internal control and poor supervision by Société officials Unhealthy corporate culture	Jérôme Kerviel (Individual)	Lonely, very ambitious and authorized trader Eagerness to progress and advance Make profits for the bank	- Abuse of forgery and trust in Société IS - Observation of financial rules for trespassing them - Taking speculative positions on stock market	€ 4.9 billion losses	2008
Pescanova	Lack of internal control over associations and poor supervision of Chairman activities	Manuel Fernández de Sousa, Pescanova Chairman (Individual)	Recognized businessman with many contacts worldwide High interest in hiding its losses.	- Creation of offshore entities, related to 'Panama Papers' - Taking his own decisions without board approval - Making stock market manipulation in relation to its own shares	$ 3.28 billion losses	2012

Table 2: *Analysis of Cases about Accounting Fraud & Financial Cybercrime: Companies' Weaknesses, Originators of Fraud, Causes for committing it, Fraud Strategy, Economic Losses and Year of Occurrence. Source: Own elaboration.*

It is noticeable that all cases presented in the table above show internal fraud, i.e. carried out by employees of the organization; while Enron and Pescanova are not only internal fraud cases since they were also supported by external auditors from Arthur Andersen, and BDO respectively.

❖ **Enron**

Enron Corporation, the largest power distribution company, led to bankruptcy in October 2001 when the Arthur Andersen failure audit was uncovered through an exhaustive investigation by the US Securities and Exchange Commission (SEC).

Arthur Andersen was one of the five largest audit and accounting firms in the world until this scandal came to light. So far, Arthur Andersen was auditing Enron accounting for 16 years.

Enron developed a team of executives who were able to hide billions in debt from failed deals and projects. In order to hide them, managers took advantage of accounting loopholes, special purpose entities and poor financial reporting.

Andersen auditing was suspected of having destroyed compromising documents, in which Enron had camouflaged its precarious financial situation, specifically losses that reached $ 63.4 billion. Its liabilities amounted to more than $30 billion. Apart from that, the Enron scandal was the largest bankruptcy reorganization in US history. Enron employees and shareholders received limited returns in lawsuits, despite losing billions in savings, pensions and stock prices.

In October 2002, Arthur Andersen was fined $500,000 and sentenced to five years of probation for obstruction of justice in connection with its handling of Enron documents. (The New York Times, 2002) Arthur Andersen's relationship with its customers was seriously injured, losing 650 of its 2,300 public sector customers in the US and others abroad. (La Nación | El Mundo, 2002)

The causes of this scandal were incentives to managers. They earned huge bonuses if they increased profits at all costs. (Silverstein, 2013)

Some of the lessons we can learn from Enron scandal is that there must be a clear mission and a code of ethics that is inculcated to its employees. Teamwork is very important, so employees do not focus on their own interests and profits but the enterprise's success. However, employees have to cooperate without violating the corporate codes of conduct established. Rationalization of individuals can be affected wrongly in a teamwork environment if employees have in mind that 'the whole team is participating' in the fraud, and therefore, are subject to some peer pressure that leads them to commit fraud.

Besides what discussed above, it is evident that managers and auditors had access controls to hide information or alter records in their financial reports. In the next section, it will be explained the legislation that emerged in the wake of the Enron scandal: Sarbanes-Oxley Act of 2002 (SOX).

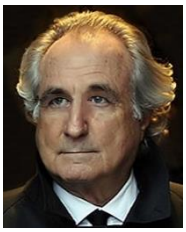
❖ **WorldCom**

The telecommunications corporation WorldCom, now known as MCI, Inc. was the United States' second largest long distance telephone company, after AT&T. WorldCom experienced rapid growth in the 1990s by acquiring other telcom companies, such as Williams Telecommunications Group Inc for $2.5 billion and MCI Communications Inc. for $40 billion. After 65 acquisitions, the company was very competitive and WorldCom's stock was trading above $64 per share.

This company's growth came to a halt when fraudulent accounting methods were uncovered. In 2002, WorldCom incurred in operating costs (mostly costs associated with using outsourced network services, called "line costs") that were posted wrongly as capital expenditures on the balance sheet instead of expenses. (Universia Knowledge@Wharton, 2003) Moreover, Worldcom granted large personal loans to the CEO Bernie Ebbers totaling around $400 million. All these transfers were not in accordance with generally accepted accounting principles (GAAP). The SEC filed fraud charges against WorldCom. At that time, stocks were trading around $15 per share. Auditors' investigations revealed $3.8 billion worth of fraud, being thus the second largest accounting fraud in American history.

Regarding to the causes of fraud assessed earlier, WorldCom CEO received $7.5 million in bonuses in 1999 and CFO, Scott Sullivan, $2.76 million, when the company was not making profits. Incentives were not measured by performance goals and this was a very strong motivation for CEO and CFO to commit fraud. Top management and accounting employees who committed fraud could override internal controls to commit fraud, so opportunity evidently existed.

❖ **Bernie Madoff scandal**



The Madoff investment scandal is the major case of stock and securities fraud discovered in United States. Bernard L. Madoff, founder and CEO of Madoff Investment Securities (BMIS) and one of the most active investors in the last 50 years, was the sole author of one of the biggest financial scams. In late 2008, Bernard Madoff was arrested by FBI after admitting that his business was a large 'Ponzi scheme' that had caused $50 billion losses to customers. In June of 2009, Madoff was sentenced to 150 years in prison. (Calvo, 2013)

A Ponzi scheme is a pyramidal fraud investment operation: the promised return to investors is paid from new capital paid by the entry of new customers. The scheme was named after Charles Ponzi notorious technique in 1920, which was closely followed by Bernie Madoff.

In order to operate with so many investors, Madoff convinced them "using" a split strike strategy[2], so it was possible to make money in both rising and failing markets. (Análisis Global, 2009) This attractive and exclusive product along with Madoff reputation for being co-founder and ex-president of the board of the US Nasdaq index (one of the most important stock indexes in the world) was spread by word of mouth among the wealthiest millionaires and investment banking.

In this case, this financial scam is caused by low risk benefits which are really secure and a prestigious investor. His image and authoritative position is a source of capability of fraud, and his Ponzi scheme evidences the lack of internal control procedures in BMIS, so opportunity exists.

❖ **Jérôme Kerviel**

Jérôme Kerviel is the personification of financial scandal in France. Kerviel is an ambitious young trader of modest origin who was working in the French bank Societé Générale for 8 years. Société Générale is one of the main financial services' companies in Europe.

In January of 2008, he was sentenced to five years in prison and to repay 4,900 million euros to Société Générale for taking speculative positions on the stock market that caused a large hole in the accounts of the entity. In addition, in 2012, Kerviel was convicted of abuse of trust, forgery and fraudulent introduction of data into the computer system of Société Générale. (Benito, 2012)

In march of 2014 after several trials, the French Supreme Court changed the sentence of three years in prison for Jérôme Kerviel and decided to cancel the huge compensation of 4,900 million euros that the bank requested to Kerviel. (Mora, 2014)

Kerviel started his financial tricks buying amounts of shares of a company in Tokyo or Hong Kong and then sold them immediately in Paris or New York taking advantage of very small price differences. Later on, he tried to hide bad investments in risky products. He bought large blocks of shares, withheld them and sold them when rising markets. Kerviel concealed the risks taking inverse operations with fake counterparts. Because of the financial crisis and falling markets, he was not able to sell them so he embarked in the futures market, betting he was going to sell huge

[2] Split strikes conversions involves buying stocks of large companies, and also buying and selling options of those same securities. This strategy was not actually followed by Madoff, but the strategy he told all his investors he was carrying out.

number of shares in a determined period, until he was discovered committing 50,000 million euros in the unstable futures market.

However, Kerviel maintained his innocence during the trial and confessed that his managers knew these operations at all times, stating that he was the patsy so he claimed responsibility to Société officials for bank losses.

This is a case where opportunity definitely existed. Gauls securities regulators fined €4 million to Société for serious shortcomings in the system of internal control. Additionally, his capabilities as an authorized trader in the Société system helped him to conduct this fraud. He observed during years the controls to break the financial rules and hide shares. When he broke the rules, his rationalization changed. He thought of the bank day and night and changed his life, left his girlfriend... Fraud changed his behavior. Kerviel eagerness to progress and advance to the first line of the bank, along with the lack of review and control of his managers made the fraud occur.

❖ **Pescanova**

The last enterprise affected by fraudulent financial operations is Pescanova. Pescanova is one of the world's largest fishing groups, founded in Spain in 1960 by José Fernández López. The Pescanova group currently operates in 24 countries over the 5 continents. Pescanova was an example of successful vertical integration, controlling all stages in the supply chain.

The main character of this case is Manuel Fernández de Sousa, Chairman of Pescanova when the scandal broke. He inherited the company that his father (Jose Fernandez Lopez), a successful and influential businessman and entrepreneur in Madrid and Galicia, built up. Sousa stood out for a superior education level (studied abroad a senior management course) and a high ability for social relations. His capabilities as a recognized manager and Chairman were unquestionable.

However, he also had conflicts with many people since he was so important that he only spoke with exclusive managers or presidents. This was the main reason he took his own decisions without taking into consideration the executive team, the board of Pescanova and even his family, who were also placed in management positions in the group's subsidiaries. This was one of the main failures in the company, the capability of its Chairman to take decisions without approval of the board of directors. Undoubtedly, the Chairman user had higher privileges in the system and it was not well controlled and regulated.

The risky decisions that Sousa carried out were uncovered in 2012, in the annual report that the BDO, Pescanova's auditing firm, published. One of Pescanova shareholders filed a lawsuit against BDO, which was charged for an alleged crime of falsification of economic and financial information. Specifically, BDO reported losses amounting 1,483 million euros, when the actual amount reached 2,700 million euros.

Then, the company suspended its auditors BDO and hired KPMG to carry out a forensic analysis of its accounts. (Reuters, 2013). Pescanova revised its balance sheet of 2012 and recognized that kept *double accounting*. Pescanova stated that the accumulated 1,850 million euros of debt was distributed among Spanish subsidiaries, foreign subsidiaries and in the core company in Galicia. Adding up commitments and debts to suppliers, the real figure of debt amounted about 4,000 million euros (approximately 4,469 million dollars), almost 4 times what was initially recognized.

In addition, Sousa revealed that before the firm scandal when Pescanova shares were trading highly (between 13.45 to 17.99), he sold his 7.2 percent stake in the firm. Approximately, he could have raised at least 27 million euros. (Reuters, 2013) Due to this fact, the National Securities Market Commission (often abbreviated as CNMV) imposed fines to Pescanova for a total amount of 450,000 euros and to its executive president Manuel Fernandez de Sousa 225.000 euros for violations of the Law on Securities Market. (La Voz de Galicia, 2015)

KPMG certified that Pescanova operated with a large group of offshore companies spread over all kind of tax havens (El Confidencial, 2016). Recently, the information collected from the "Panama papers" detected that Sousa actually created offshore entities through a Panamanian law firm (Mossack Fonseca) in British Virgin Islands. These entities were registered in this tax haven to hide the identity of its owner (Sousa) and for avoiding taxes, paying a very low rate or not paying at all.

After Pescanova bankruptcy in 2013, Sousa requested urgently to Mossack Fonseca a certificate proving that his companies were disabled and all its assets belonged only to himself, so he could exculpate the other members of the board of Pescanova (infoLibre, 2016)

Despite Sousa amendments, he was obviously fired from the company. The company changed its top management and was restructured under a new company brand, "Nueva Pescanova".

3.3 Cybercrime: Fraud & Security Breaches

Fraud in cybercrime is not only related to accounting problems as the cases we have reviewed above. The computers, information systems or access controls of an enterprise can be compromised to exploit security holes. This is the scenario of cybercrime that takes the *'computer as a tool'* to commit fraud.

Cyberattacks and security

Nowadays computer security suffers threats that result in many cases in huge economic losses. Thefts of corporate information cannot only undermine confidence in the enterprise, but jeopardize its economic survival.

Based on a recent research (CISCO & BT, 2016), these are some shocking figures about security attacks:

- 169 million of entities were theft only in 2015.
- 300 million of malware files are created yearly.
- 97% of Fortune 500 enterprises have been hacked.
- Every 2 seconds there is an identity theft in the US.
- Cyberattacks increase on an annual 48% basis.

Cybersecurity is not anymore a one-time strategy performed to avoid possible attacks. Companies cannot underestimate the possibility that a major attack happen to them, because attacks are getting more intense and sophisticated, and online information theft is currently very strong. For this reason, companies must be fully involved in the security standards deployed, since cybersecurity is a "permanent process which seeks to eliminate weaknesses, and to be more intelligent than the attacker", as described by a Rand Corporation study published in 2015. Cybersecurity is a continuous process where departments such as risks, security, internal control… have to work and collaborate together to develop security at all levels.

3.3.1 Security Breaches Cases

Over the last 10 years, some relevant cases have stood out due to the vast amounts of information hacked. All these data breaches recorded are reported in 2004 or beyond, mainly since the rapid growth of data. This fact gives cyber criminals more opportunities to expose massive volumes of data in a single breach.

Before analyzing every case in further detail, in the following table there is an overview of the cases being reported and some relevant features about them, such as:

1. Name of the company affected by fraud
2. Weaknesses of the company affected by fraud, which are company's failures that facilitated fraud to occur

3. Name of the originator of fraud specifying if it was committed by an individual or a collective (the company to itself or a third party group)
4. Leak method developed regarding to cyberattacks (**Cases have been documented and sorted by this factor)**
5. Fraud strategy: Action plan to carry out fraudulent operations
6. Economic or data losses that resulted from fraud
7. Year of occurrence of the case described

Company affected	Company's weaknesses	Originator of fraud	Leak method	Fraud strategy	Economic or data losses	Year
AOL	Lack of access control tools, poor security of critical customer data	Jason Smathers: Individual	Inside job	- Access to critical data using other employee credentials - Selling millions of customers' email addresses to spammers	92 million screen names and email addresses stolen	2004
Court Ventures	Lack of access control tools, poor security of critical customer data	Court Ventures: Collective	Inside job	- Access to critical data stored in a third-party database (US Info Search) - Reselling consumer data to a Vietnamese ID thief	200 million consumer records sold (SSN, credit card data, bank account data)	2012
T.J.Maxx	Weak WEP encryption of data in the stores system	A hackers' band: Collective	Hacking	- Packet sniffer installed on the network which collected real-time data & payment info - Stolen data sold to ID thieves	94 million of Visa and MasterCard accounts exposed	2007
Heartland Payment Systems (HPY)	Poor protection of sensitive data against SQL injection attacks	Unknown intruders: Collective	Hacking	- Sniffer malware installed in the HPY application - SQL injection attacks that read customer data	134 million credit card holder data, SSN stolen; $110 million paid for claims	2008
EBay	Employees' unconsciousness of security and the risk that pose ID credentials	A group of hackers: Collective	Hacking	- Obtained login credentials from a group of employees - Accessed a consumer records' database and changed their credentials	145 million users' passwords had to be changed since they were modified	2014
SWIFT	Insufficient banks' internal security measures	'Lazarus', a hackers' band: Collective	Hacking	- Stole credentials to order illegal transfers from Bangladesh Bank reserves to accounts in Philippines. - Malware on Alliance Access network	$81 million stolen to the Bangladesh Central bank reserves	2016

Table 3: *Analysis of Cases about Cybercrime & Security breaches: Companies' Weaknesses, Originators of Fraud, Leak method, Fraud Strategy, Losses and Year of Occurrence. Source: Own elaboration.*

❖ **AOL**

In 2004, Jason Smathers, a software engineer in America Online Inc., stole 92 million[3] screen names and email addresses using another employee's access code. The stolen list included multiple email addresses of AOL customers in 2003 in Virginia. He then sold this information to spammers who sent out unwanted gambling advertisements to AOL subscribers, specifically up to 7 billion unwanted emails. This case could have been prevented using appropriate techniques for access control.

❖ **Court Ventures**

In March 2012, Experian (the US leading global information services company that provides data and analytic tools) acquired Court Ventures (Lord, 2015). Court Ventures is a company that focuses on collecting court records which contain personally identifiable information (PII). One of Court Ventures' subcontractors was US Info Search, with whom Court Ventures customers could find people addresses to determine which court records to review. The US Secret Service notified that Court Ventures was reselling data from a US Info Search database to a third party: ID thieves like a 25-year-old Vietnamese man, Hieu Minh Ngo, among others. (Krebs on Security, 2015) 200 million[4] consumer records including Social Security numbers, credit card data and bank account information were compromised.

In the previous cases, the leak method used was performed inside the company, either by a former employee who committed **identity theft** to access to consumer data in order to sell it, or by a company that permits the **sale of third party's data** to an identity thief. These cases are examples of '*inside job*' as a leak method. These scenarios show how some employees compromised information by inappropriate access to critical data.

T.J.Maxx

TJ Maxx breach is the largest retail breach to date: 94 million[5] of Visa and MasterCard accounts were exposed to potential fraud. T.J.Maxx is an American department store chain with more than 1,000 stores. T.J.Maxx infringement occurred because of a weak WEP encryption in use in two of its Marshalls stores in Miami. Once intruders had access, they installed a packet sniffer on the T.J.Maxx network, which collected data from real-time operations, including data stored on payment cards. Thus,

[3] 92 million screen names and email addresses stolen, figure contrasted among different sources: (NBC News, 2005) (The Washington Post, 2004) (WIRED, 2004)
[4] 200 million consumer records compromised, figure contrasted among different sources: (Experian, 2014) (Krebs on Security, 2015)
[5] 94 million of credit card accounts exposed, figure contrasted among different sources: (ABC News, 2007) (NBC News, 2007) (The New York Times, 2007)

hackers were able to appropriate data of millions of customers. The hackers band used some of the account numbers stolen for personal use while others were sold to other international data thieves.

The fraud committed by T.J.Maxx highlighted the increased vulnerability to theft of personal information. T.J.Maxx case which occurred in 2007 was one of the largest scandals before the cases mentioned above, such as Heartland, eBay, Court Ventures…

❖ **Heartland**

Heartland Payment Systems (HPY), a leading payment processing company, is recognized as the largest credit card scam in history. This attack happened in 2008 when Heartland systems were compromised by a sniffer malware. 134 million[6] credit card holder names and numbers as well as Social Security numbers were exposed through SQL injection attacks.

Heartland paid more than $110 million to Visa, MasterCard, American Express and other card associations to settle claims related to the breach. (Pepitone & Remizowski, 2012) Then, HPY informed about this breach to cardholders and advises them to analyze their monthly statements to prevent any suspicious activity.

Unknown intruders used SQL injection attack, which consists of insertion of a SQL query via data input or transmitted from the client to the web application. This attack enables to read sensitive data from a database, modify data, execute admin operations, and so on.

❖ **eBay**

A group of hackers attacked the company between late February and early March in 2014. They obtained the login credentials to access from a small number of employees. Then, they accessed an enterprise database which contained all users' records and copied some of these credentials. Exactly 145 million[7] users were affected and were forced to change their passwords. After this scandal came to light, eBay shares fell to their lowest value of the last 2 years.

This cyberattack led by a hacker group took advantage of an enterprise weakness: employees of the company. In other cases, hackers exploit hardware or software weaknesses, however, employees are a major cause of attacks. Enterprises usually

[6] 134 million credit card holder names and numbers and SSN exposed, figure contrasted among different sources: (COMODO, 2013) (Bloomberg, 2009) (PCADvisor, 2012)
[7] 145 million users affected, figure contrasted among different sources: (Reuters, 2014) (Business Insider, 2014) (The Washington Post, 2014)

do not make employees conscious of the importance of their credentials, passwords or the data they manage, which is critical for hackers or any identity thief.

- **Bangladesh Bank & SWIFT**

In the last case presented regarding to cybersecurity, the main character is Lazarus, the most sophisticated hackers' band in the world. Since 2009, Lazarus is linked to a series of cyberattacks targeting US and South Korean organizations (Global Cybersec, 2016). This North Korean band is specialized in executing fraudulent transactions over the SWIFT network. This is why Lazarus is the major suspect of the largest cyber heist in history, occurred in Bangladesh Central Bank.

Hackers planned an ingenious strategy to attack the global financial messaging system that secure interbank operations: SWIFT. Approximately 11,000 financial institutions use the SWIFT (Society for Worldwide InterBank Financial Telecommunications) financial platform. Additionally, many of these banks have installed the Alliance Access software, which banks and other clients use to interface with SWIFT. (Finkle, 2016)

Last January, this group of hackers took advantage of some weaknesses of Alliance Access software and intrude into the Bangladesh Central Bank's systems. Once they accessed, they stole its credentials to execute payment transfers. They sent 35 SWIFT requests to the Federal Reserve at New York in order to transfer Bangladesh Central Bank funds to accounts in Philippines and Sri Lanka. The initial robbery involved an amount of $951 million. $101 million were actually transferred, but the remaining amount was blocked by the Fed because of a misspelling in one of the transactions. An order to 'Fandation Shalika' instead of 'Foundation Shalika' ruined the fraud, since the Federal Reserve could not find a bank with the exact recipient.

US $20 million were recovered in Sri Lanka bank, however $81 million[8] were hidden beneath the lax legislation existing in the Philippine casinos. These fraudulent transfers were covered up through the malware implemented and distributed.

EBay, Heartland, T.J.Maxx and Bangladesh Central Bank were cases where the method of leak was **hacking**. Hacking methods like installing packet sniffers or SQL injection are more sophisticated examples than just using employee's credentials like in eBay. These cases deployed **phishing** techniques since they 'harvest' personal information such as ID credentials, credit account numbers and passwords... to commit fraudulent operations.

[8] 81 million of credit card accounts exposed, figure contrasted among different sources:

However, all these cases show weaknesses of the companies affected that hackers exploited to compromise data and jeopardize the enterprise survival causing poor brand image, distrust, huge economic losses…

As consequence of these significant cases where fraud and cybercrime have been notable, there is an important effort of governments to regulate these scandals, so companies can prevent them whether they occur because of an inside job or external factors such as cyberattacks through hacking, phising, sniffing and so on.

3.3.2 Cost of Implementation of Security Measures to prevent breaches and fraud

Regarding to the security cases analyzed above, there have been collected some solutions that could help companies to prevent fraud and security breaches.

In the table below, there have been captured the failures of these companies, fraud strategy and their losses, represented in 2nd, 3rd and 4th columns (also previously exposed in Figure 13). In the 5th column, there are have been considered some security measures that could be acquired by a company in order to avoid any future failure regarding to its security holes. These could be used as examples for other enterprises that face similar weaknesses. In the 6th column, there have been listed the costs that should be incurred.

Costs of these measures not only depend on the enterprise size, but the security system already installed in the company, the applications involved for its business processes, the web tools installed for controlling access and users' privileges and the number of users that access the system, among others.

The tool that is being analyzed in this thesis for access control and regulate internal policies and risks is SAP GRC Access Control. This tool enables to reduce intrinsic risks in business processes, create automatically alerts when risks are detected, implements remediation controls for risk violations, checks mandatory compliance over risk mitigation, automates user access, role authorizations, and so on.

However, in the following table, there has been noted another system for protecting our data and securing information, IBM Security Guardium. This product guarantees security, privacy and data integrity in the enterprise data center. It enables data encryption and other tools for classification of sensitive data and alerts when there have been data changes or intruders in the system.

	FAILURES AND LOSSES ASSOCIATED			SECURITY SOLUTIONS AND THEIR COSTS	
Company affected	**Company's weaknesses**	**Fraud Strategy**	**Economic or data losses**	**Security measures**	**Implementation cost of these measures**
AOL	Lack of access control tools, poor security of critical customer data	Access to critical data using other employee credentials Selling millions of customers' email addresses to spammers	92 million screen names and email addresses stolen	Web Access Control Authorization architecture in the enterprise security system (SoD[9] model) Data privacy system	Cost of a similar tool to SAP GRC Access Control and its implementation Cost of a similar tool to IBM Security Guardium
Court Ventures	Lack of access control tools, poor security of critical customer data	Access to critical data stored in a third-party database (US Info Search) Reselling consumer data to a Vietnamese ID thief	200 million consumer records sold (SSN, credit card data, bank account data)	Web Access Control Data privacy system Authorization architecture in the enterprise security system (SoD model)	Cost of a similar tool to SAP GRC Access Control and its implementation
eBay	Employees' unconsciousness of security and the risk that pose ID credentials	Obtained login credentials from a group of employees Accessed a consumer records' database and changed their credentials	145 million users' passwords had to be changed since they were modified	Web Access Control Data privacy system Authorization architecture in the enterprise security system (SoD model) Security Awareness and Training Policy	Cost of a similar tool to SAP GRC Access Control and its implementation Cost of a similar tool to IBM Security Guardium Cost of Security Awareness Training Courses
Heartland Payment Systems (HPY)	Poor protection of sensitive data against SQL injection attacks	Sniffer malware installed in the HPY application SQL injection attacks that read customer data	134 million credit card holder data, SSN stolen; $110 million paid for claims	IDS implementation to detect any sniffer malware Data privacy system Database protection procedures to prevent SQL attacks	Cost of an IDS deployments Cost of a similar tool to IBM Security Guardium

[9] SoD is referred to Segregation of Duties. This concept will be explained in further detail in the next section, specifically in section 4.2. Segregation of Duties.

T.J.Maxx	Weak WEP encryption of data in the stores system	Packet sniffer installed on the network which collected real-time data & payment info Stolen data sold to ID thieves	94 million of Visa and MasterCard accounts exposed	IDS implementation to detect any sniffer malware Data privacy system Establish WPA2 wireless network encryption	Cost of securing WiFi Cost of implementing WPA2 Enterprise Encryption on their WLAN
SWIFT & Bangladesh Bank	Insufficient banks' internal security measures	Stole credentials to order illegal transfers from Bangladesh Bank reserves to accounts in Philippines. Malware on Alliance Access network	$81 million stolen to the Bangladesh Central bank reserves	IDS implementation to detect any sniffer malware Web Access Control Data privacy system Authorization architecture in the enterprise security system (SoD model)	Cost of a similar tool to SAP GRC Access Control and its implementation Cost of a similar tool to IBM Security Guardium

Table 4: *Analysis of failures committed and security solutions that could have prevented them from occurring. Source: Own Elaboration.*

The cost of implementation and Segregation of Duties (SoD) configuration of a tool as SAP GRC Access Control depends on several factors:

- Number of business processes under the enterprise management (this is referred in this case to SAP modules). The cost will vary depending on the number of SAP modules implemented in the enterprise, since more modules signify more SoD conflicts to analyze.
- Number of users that access the system (SAP or other applications).
- Type of system where the security architecture is implemented: SAP or non-SAP system. If the access control structure is configured on a non-SAP application will require more time and effort to make it work properly and streamlined with SAP GRC AC.
- Number of transactions executed per year in SAP, or in other applications

These various factors can be interpreted as variables for our cost analysis:

Variable X: Number of business processes. X is unknown, it cannot be known which business processes are carried out under the enterprise management or which processes are outsourced.

Variable Y: Number of users that access the system. Y could be estimated as the number of employees in the firm.

Variable Z: Type of security system used. Z is also unknown, since it cannot be analyzed particular systems that the enterprises reviewed actually use.

Variable K: Number of transactions executed. K is also an unknown variable, since it cannot be analyzed particular systems that the enterprises reviewed actually use.

3.3.2.1 Security Software & Compliance Requirements

Considering the size of the enterprises mentioned, taking as reference the number of employees and estimating the number of transactions that can be executed in SAP, the result will be the cost of compliance with Segregation of Duties and security regulations.

If a user executes in SAP approximately 10 transactions daily and work for 260 days yearly (subtracting weekends), the number of transactions executed yearly can be calculated from the product of the latter factors. In addition, only 60% of users have been indicated as potential users of SAP GRC and other security tools.

Enterprise Affected	Number of employees	Number of employees that use ERPs and security tools (60%)	Number of transactions executed yearly
HPY	3,734	2,240.4	**5,825,040**
Bangladesh Bank	5,071	3,042.6	**7,910,760**
Aol	5,600	3,360	**8,736,000**
Ebay	11,600	6,960	**18,096,000**
Court Ventures	17,000	10,200	**26,520,000**
T.J.Maxx	198,000	118,800	**308,880,000**

Table 5: *Number of transactions executed yearly by users from the enterprises affected. Source: Own elaboration.*

When enterprises overcome 6 million transactions executed yearly, the cost of offering security compliance such as PCI for credit cards (as it could apply in the SWIFT case) amounts **$50,000 and above**.

The cost of regulation measures is related to the number of transactions executed yearly by an enterprise, as seen above.

Enterprise Affected	Number of employees	Number of employees that may use SAP GRC AC (1%)	SAP GRC Access Control License	IBM Security Guardium License	TOTAL COST of both solutions
HPY	3,734	37.34	7,430.66	3,696.66	**$ 11,127.32**
Bangladesh Bank	5,071	50.71	10,091.29	5,020.29	**$ 15,111.58**
Aol	5,600	56	11,144.00	5,544.00	**$ 16,688.00**
Ebay	11,600	116	23,084.00	11,484.00	**$ 34,568.00**
Court Ventures	17,000	170	33,830.00	16,830.00	**$ 50,660.00**
T.J.Maxx	198,000	1,980	394,020.00	196,020.00	**$ 590,040.00**

Table 6: *Security Software Solutions for the enterprises affected by security breaches. Source: Own elaboration.*

Estimating a SAP GRC Access Control license for 1 user yearly for the amount of $199, it can be then calculated the cost of these licenses for all users that require access to this tool in every company reviewed. IBM Security Guardium license for 1 user amounts $99 yearly, based on cost estimations in comparison with other IBM Security products.

In the table above, it has been estimated that only 1% of users in the company will require access to this tool, since it is mainly used by a reduced group of Security Administrators and some employees from the Internal Control & Fraud, and Risks departments.

3.3.2.2 Personnel Costs

In order to provide a complete SoD architecture based on risks and adjust in a tool as SAP GRC Access Control, it is required a group of security consultants, analysts and support members (among others) working on this project. The total cost of this team amounts a total of **$529,464.00** for a period of time of **3,120 hours** (40 hrs/week): 78 weeks, approximately **lasting 1 year and a half.** This is the average duration of these projects.

Job position	Number of Members	Cost/hour ($)	Number of hours	Total Cost ($)
Analyst of Business Processes	2	56.00	936	52,416.00
Fraud Risks Consultant	1	51.00	624	31,824.00
IT Security Technical Consultant	2	62-00	1,560	96,720.00
SAP Functional Consultant	1	51.00	936	47,736.00
IT Security Support members	3	39.00	1,872	73,008.00
Project Manager	1	73.00	3,120	227,760.00
	10		**3,120**	**$ 529,464.00**

Table 7: *Personnel costs for a SoD project. Source: Own elaboration.*

3.3.2.3 Total Costs

The total costs of the software solutions cost and the personnel cost contracted for this project would determine the total cost shown in the last column, which ranges from $590,591.32 in the case of a 'smaller' company as HPY to $1,159,504 in the T.J.Maxx case, which represents a very large company.

Enterprise Affected	Regulations Compliance	Software Cost	Personnel Cost	TOTAL COST
HPY	$ 50,000	$ 11,127.32	$ 529,464.00	**$ 590,591.32**
Bangladesh Bank	$ 50,000	$ 15,111.58	$ 529,464.00	**$ 594,575.58**
Aol	$ 50,000	$ 16,688.00	$ 529,464.00	**$ 596,152.00**
Ebay	$ 50,000	$ 34,568.00	$ 529,464.00	**$ 614,032.00**
Court Ventures	$ 50,000	$ 50,660.00	$ 529,464.00	**$ 630,124.00**
T.J.Maxx	$ 50,000	$ 590,040.00	$ 529,464.00	**$ 1,159,504.00**

Table 8: *Total Costs of Security Measures proposed. Source: Own elaboration.*

Additionally, companies should always implement systems for protecting data so in case of a disaster, failures, data thieves, or compromise of data by fraudsters, data can still be recovered. In the event of these critical situations, data could be available by using **backup systems**. Data availability is a key issue nowadays, so it is important that companies take into account systems that ensure accessibility and availability whenever it is needed.

In the same way that information systems are usually contracted through software licenses, backup systems use this contract method too.

In order to estimate the cost of the implementation of a backup system in an enterprise, there are some factors to be considered:

- Size of the enterprise
- Network sockets
- Number of clients running on the front-end server
- Number of applications to be protected

In the total costs proposed above, there has not been included the amount of budget for backup systems. This is an additional service, but not required for a Segregation of Duties project.

3.3.2.4 *Cost of Security Solutions as percentage of the Losses in Security breaches*

In order to calculate total losses, there have been considered two factors: number of records stolen and sold and its cost in the market.

Based on results from the 2015 Cost of Data Breach Study: Global Analysis, the average cost of a data breach hits $154 per stolen record. (IBM, 2015)

The product of the number of data records compromised and the average cost of it, $154 (plus additional losses, if applied) results in total losses, represented in the 5th column of the table below.

Enterprise Affected	Total Cost of Security Measures in dollars (1)	No. Data records compromised	Additional Losses, in dollars	Total Losses, in dollars (2)	PROPORTION (1/2)
HPY	$ 590.591,32	134000000	110000000	20746000000	**0,00285%**
Bangladesh Bank	$ 594.575,58		81000000	81000000	**0,73404%**
Aol	$ 596.152,00	92000000		14168000000	**0,00421%**
Ebay	$ 614.032,00	145000000		22330000000	**0,00275%**
Court Ventures	$ 630.124,00	200000000		30800000000	**0,00205%**
T.J.Maxx	$ 1.159.504,00	94000000		14476000000	**0,00801%**

Table 9: *Proportion of the cost of security measures against losses caused by security breaches. Source: Own elaboration.*

In the case of Bangladesh Bank and Swift, the cost of implementing security measures as SAP GRC Access Control (acquiring software licenses and the personnel to implement this project) and IBM Security Guardium represents only **0.73404%** of the losses that this scandal provoked.

Furthermore, in the losses represented above, there have not been included other costs resulting from the breach such as brand image losses or lawsuits costs.

As can be seen in the table above, the magnitude of costs incurred when carrying out security projects based on segregation of duties is negligible and has an extremely small value in relation to the costs involved in security data breaches where large numbers of customer records are involved.

4 FRAUD-PREVENTION STRATEGIES

In light of the existence of numerous cases in which financial fraud through cyberattacks and malware is in vogue, strategy solutions have been developed to prevent fraud.

On one hand, in the governmental framework, there are many **regulations** that have arisen in order to define rules and standards for internal control governance in corporations all over the world, such as SOX in the US, or SCIIF (ICFR) in Spain.

On the other hand, from a more technical point of view, there must be established some **security solutions** to prevent fraud. Firstly, recognizing which risks are more relevant in our company, and which risks result from different tasks carried out by the same person or department. Then, a key point is to analyze its impact and probability, thus, mitigate them and set up prevention measures, and a contingency plan.

The solution proposed to prevent fraud in this thesis is based on the concept of **segregation of duties** in the company followed by a proper analysis and **risk assessment**.

Regardless of the technical strategy used by our company to prevent fraud and other critical risks, this solution must comply with the rules in force in every country with respect to internal control and corporate governance.

4.1 Applicable Regulations

In order to establish certain rules on how companies have to regulate their processes and the activities performed in the organization, some regulations provide accurate information about Internal Control and Corporate Governance. The most innovative regulations regarding to Internal Control were Sarbanes-Oxley Act and COSO regulation.

4.1.1 COSO: Internal Control Objectives, Components and Levels

COSO, Committee of Sponsoring Organizations of the Treadway Commission, is an initiative to improve internal control within organizations.

Despite COSO is not as popular as SoX, COSO provided a very solid integrated conceptual structure, which has become the main standard in the world.

A concept that is being used throughout any corporate control regulation is *Internal Control*. According to COSO (McNally & CPA, 2013), “Internal control is a process effected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives (…)”.

The three different categories of objectives are:

- Effectiveness and efficiency of operations
- Adequacy and reliability of financial operations
- Compliance with applicable laws and regulations

Thus, Internal Control is an objective-oriented process that is conceived and executed by people at all levels of an organization.

Furthermore, internal control consists of repetitive and permanent processes that are integrated together into a dynamic system that is affected by changing business conditions. These multidirectional processes that compose Internal Control are:

1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information and Communication
5. Supervision and Monitoring

4.1.2 Fraud Scandals' Legacy: Sarbanes-Oxley Act

A number of corporate accounting scandals created a need for regulations, such as the US Sarbanes-Oxley Act.

US Sarbanes-Oxley Act of 2002 commonly called **Sarbanes-Oxley, or SOX**, is a United States federal law enacted on July 30, 2002 in response to a number of major corporate and accounting scandals such as Enron, WorldCom, Tyco, Adelphia, Xerox and the other scandals mentioned above. This legislation emerged mainly in the wake of Enron, exactly 15 months later from the uncovering of Enron Scandal on October 2001.

SOX was developed by the famous auditors: Paul Sarbanes, a democrat US Senator in Maryland, and Michael Oxley, a republican US Senator in Ohio.

SOX aimed to re-establish investor confidence regarding financial information issued by companies, which should have been audited professionally following these security standards.

The introduction to SOX states that this act was an act intended 'to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes'. (Sarbanes, 2002)

SOX Compliance is applicable to all companies listed on New York Stock Exchange, whether it is listed the entire company, or a subsidiary.

Compared to COSO concept, SOX adds two new elements: audit of internal control and COSO organizational perspective.

Internal control structure, as defined by SOX, is segregated into three different levels of control and their respective officers:

1. Structures and Internal Control Procedures: This is the broadest internal control level, for which the administration is responsible for: establishment and maintenance; and assessment of internal control effectiveness.
2. Internal Accounting Controls: This a technical level referred to the process of financial reporting. Auditors are responsible of the auditing reports.
3. Internal Controls: This is a more practical level associated to the effectiveness of solving problems that are faced on a daily basis in organizations.

Some of the sections reviewed below are *Section 302*, which is listed under Title III of the act, and pertains to 'Corporate Responsibility for Financial Reports'; and *Section 404*, which is listed under the Title IV of the act and pertains to 'Management Assessment of Internal Controls'.

4.1.2.1 Section 302:

The CEO/CFO Must Certify Quarterly and Annually that:

- The Securities & Exchange Commission report has been reviewed by the CEO/CFO
- The report does not contain any misleading and/or untrue statements
- Significant deficiencies and material weaknesses in internal control have been disclosed to the Audit Committee and auditors, as well as any fraud (material or not) involving anyone with a significant role in internal control
- Material weaknesses must be disclosed in the annual report to shareholders

Section 302 is very important since it forces top officials of public companies to be aware, knowledgeable and responsible of fraud or any error in their internal control systems. Top executives are legally accountable for the financial information disclosed.

4.1.2.2 Section 404:

Defines the rules for internal control and financial reporting

- Companies that must comply with SOX must assess effectiveness of internal control structure and procedures for financial reporting
- The responsibility for establishing and maintaining adequate internal control over financial reporting lies in the management

- Material weaknesses in internal control over financial reporting must be identified by management
- External auditors shall attest to and report on management's assessment of internal control for financial reporting.

Through effective Internal Controls over Financial Reporting (ICFR), the right rules are established to provide reliable financial statements. (Sarbanes, 2002)

Section 404 and section 302 are closely related, because Section 404 explains how to implement internal controls so we can prove what management has been required to review and certify, based on section 302.

On the other hand, Section 401 addresses fraudulent actions in companies, and aims to discourage the use of fraudulent tactics that involve off-balance sheet items. In case of substantial changes in their financial situation, companies have to communicate immediately these variations publicly, according to Section 409.

To sum up, SOX changed corporate governance in different ways:

1. It made corporate board of directors aware and responsible of any fraud or error in the internal control systems
2. It imposed audit requirements over how companies regulate internal control
3. It reinforced and promoted the creation of codes of ethics
4. It created new responsibilities, that entailed additional costs on public companies and accounting firms
5. It led to a greater internal control of financial reporting and made financial reporting to be certified and audited
6. It originated a new regulator: Public Company Accounting Oversight Board (PCAOB) to establish and reorganize auditing standards based on risks
7. It made companies respect and comply with corporate governance

4.1.3 Regulation for Internal Control and Corporate Governance Systems

The regulation that is applied in Spain regarding to internal control in regulated entities are the following:

- *Internal Control over Financial Reporting* in listed companies (**ICFR**) system issued by COSO, or **SCIIF** in Spanish: Sistemas de Control Interno de la Información Financiera. This regulation was implemented by CNMV (Comisión Nacional de Mercado de Valores).
- Internal Control of management companies of *Undertakings for the Collective Investment in Transferable Securities* (**UCITS**). This relates to investment funds regulated at European Union level.

In Spanish, UCITS is defined as **SGIIC**: Sociedades Gestoras de Instituciones de Inversión Colectiva y sociedades de inversión.

- Internal Control Audit for Service Providers: International Standard on Assurance Engagements (**ISAE 3402**, *Assurance Reports on Controls at a Service Organization*), which substitutes the Statement on Auditing Standards 70, Service Organizations (SAS 70). The US standard applied is **SSAE 16**: Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization.
- Sectoral regulation for internal control, such as:
    - **Solvency II** is a European directive aimed at regulating the activities of *insurance and reinsurance*, homogenizing the European legislative landscape.
    - **Basilea III** is a global regulatory framework to strengthen the governance, supervision and risk management of the banking sector, drawn up by the Committee on Banking Supervision.
- Advice on the implementation of *Markets in Financial Instruments Directive* (**MiFID**). It regulates organizational requirements including internal control such as compliance, internal audit and risk control.
- Advice when taking control of the *Foreign Account Tax Compliance Act* (FATCA). Organizations should focus on designing governance, compliance and controls framework concurrent with the core FATCA implementation effort.
- Compliance with the Sarbanes-Oxley (SOX), specifically EuroSOX, the scaled version for Europe. SOX also has other versions such as CSOX (in Canada) and JSOX (in Japan).

On the other hand, to establish security controls in corporative governance, the following regulations must be followed:

- Advice and review of the Annual Report of Corporate Governance (EPCM).
- Compliance with the Code of Good Governance and information systems to third parties
- Compliance with Corporate Social Responsibility, defined in the ISO 26000
- Implementation of good governance practices of Information Systems COBIT, ITIL, ISO 27000, etc.
- Ethics and integrity programs and development of codes of conduct
- Implementation of the Center for Internet Security (CIS) controls
- Particularly in Spain, compliance with ENS (Esquema Nacional de Seguridad)

4.2 Segregation of Duties

After the appearance of fraud financial cases like Enron and WorldCom and its consequent implantation of regulations applied to control as SOX, Basel III, Solvency II… it arises a wide range of fields to exploit such as new risks to address, new audit procedures to develop, new audit reports, new training for these auditors, new regulations to review, and new and changing audit standards. (Tarantino & Cernauskas, 2009)

One of the implications of these various internal controls audit standards is a greater control over application security and segregation of duties (SOD).

In this section, SOD is our main focus, since it reinterprets new standards for firms to implement in order to the prevention of fraud and errors.

Segregation of duties is a primary internal control used when undertaking financial operations, which is intended to prevent or reduce the risk of errors or irregularities, identify problems and ensure corrective action is taken (SAP Corporation). This is achieved by preventing a single individual takes control over all stages of financial transactions.

Or put more simply:

One person cannot have access to the whole process.

The task needs to be segregated so that there is check and balance.

The objective of implementing SoD in a business is to ensure that different people are involved in the different stages of a transaction so they perform different functions.

These four general categories of duties consist of: Initiation, authorization/approval, recording and settlement processes. No person should be able to record, authorize and settle a transaction.

SOD controls have to be designed and implemented taking a risk-based approach. Such controls are implemented using applications that handle accounting information or any critical information that needs to be reported. This information is usually managed in ERPs, as we explained in section 2. One of the largest ERPs in the world is SAP (See more about SAP in section 3), that's why in following sections, it will be discussed a model of segregation of duties structured in SAP.

4.2.1 Segregation of Duties Model

There are some concepts of a Segregation of Duties model that are relevant to fully understand it, such as:

- **Principle of least privilege**: users should have the minimum access to resources that are absolutely required to perform their job duties.
- **Sensitive transactions**: business transactions that potentially impact the financial statements of a company, these are usually risky operations that can affect financial statements, operating activities, or damage the corporate image.
- **SOD conflict**: the pairing of two sensitive transactions result in business risks. A SOD conflict arises from the intersection of two critical tasks, that occur or affect the company simultaneously.

The philosophy of SOD and the regulations resulted from it rely on the concept that nobody can have too many privileges to access a system and be able to execute transactions in every business process without control. This situation can pose critical risks for a business, since employees can be tempted to commit fraud or other internal control failures.

SOD can reduce the likelihood of such crimes through disseminating sensitive tasks and their respective privileges into separate roles assigned to different people or departments. In this way, users become less 'powerful' in the system.

A SOD model should accomplish two primary objectives. Firstly, SOD conflicts should be reduced to prevent the occurrence of conflicts of interest, fraud, abuse of functions… Secondly, this model should detect control failures including security breaches, information thefts, and any tactic of avoidance of security controls.

SOD conflicts result in corporate risks. An example could be a user who has privileges for two different functions, of which one comes into conflict with the other.

- Function 1: Vendor master file maintenance
- Function 2: Orders / purchases approval

These two functions will pose a risk if a user can create fictitious vendor or create an unauthorized vendor (Function 1) and make an improper purchase (Function 2).

Another example could be a user with access to these two functions:

- Function 2: Orders / purchases approval
- Function 3: Payments

These two functions will also pose a risk if a user can approve an unauthorized purchase (Function 2) and make its payment without further approval from senior management (Function 3).

A user with Functions 1, 2 and 3 could create the whole process from creating a fictitious vendor, making an illegal purchase to this fake vendor to paying it without any other approval.

For solving such conflicts, these functions should be segregated into different user responsibilities (roles). Then, each role should be assigned to only a user or a department in charge of this task. Security consultants or IT team that build an appropriate SOD structure will ensure that these separate roles are assigned to different people, and not to the same individual to avoid this risk.

For this reason, IT department and heads of different business areas should collaborate together to elaborate a complete security model that complies with SOD.

The process determined to capture, analyze, mitigate and control risks is being explained in the subsequent section.

Building a SOD model is one of the steps of a compliance lifecycle. In order to achieve SOD, IT management should establish security settings and an authorization model. Once SOD is implemented, the next step would be compliance reporting, attending to the regulations and normative related to SOD and security. This reporting would be then audited and controlled to verify that complies with the current standards. Those controls that were not be approved by the audit team should be analyzed in the next lifecycle.

Some benefits that an effective SOD model brings are saving time and money for reporting, reducing auditing costs, achieving SOX compliance, reducing risks and opportunities for fraud, and enabling a model that detects violations before being performed.

5 SOD PROCESS FROM A RISK-BASED APPROACH

Enterprises that recognize that do not know how the risk of fraud is inherent to its business processes cannot be able to develop antifraud controls to prevent it. In order to make enterprises conscious about fraud risk, an enterprise must learn to identify potential threats and the weaknesses of its controls. In this way, the enterprise will develop **continuous and frequent fraud risk assessments**.

Risk evolves and changes over time. For this reason, a company must keep pace with risk and have the agility to always assess it regardless of the circumstances of the company. The most agile way to assess risk is through a systematic assessment based on predefined **rules and automatic controls** throughout the different project phases.

The analysis of risks through a SoD analysis is being captured in the document by the risk management lifecycle illustrated below.

Figure 23: *Risk Management Lifecycle. Source: Own elaboration.*

SoD conflicts identified among two functions build up risk elements in our enterprise. The combination of all enterprise functions creates a **matrix** where we can quickly identify the crossing of these functions, thus, the risks created among them. Nevertheless, there are other combination of functions that will not pose any risk for the system.

Through this **risk identification** process, the enterprise will determine that some of these risks are not relevant for its business processes, so the response to these risks will be acceptance. However, risks that are critical and impact business processes will be analyzed, and the enterprise must respond to these risks.

The **action plan** executed to prevent these risks will depend on the materiality of risk such as the probability and its impact. In order to implement this response, it is essential that the enterprise implements **controls that mitigate** such risks.

Once mitigating controls are stablished, it comes into play the phase of reporting and **evaluating** the risks that have been eliminated, and on the other hand, **monitoring** and controlling risks that still exist and threaten our system. In this point, in order to reduce the unmitigated risks, another risk lifecycle would start.

5.1.1.1 Risk-based approach

As mentioned earlier, it is crucial to implement tasks and processes that do not create conflicts between them, since conflicts in SoD lead to risks.

According to PMI, **risk** is “an uncertain event or condition that, if it occurs, has a positive or negative effect on a project objective".

Unlike a problem, a risk is identified in advance and can occur or not; however, a problem has already occurred or is occurring, so we could not analyze it previously to have treated and evaluated this event.

Risk management (RM) “is a method of ensuring that, for a specific project, all risk events are identified, qualified and handled.” (Project Management Institute (PMI), 2013) RM aims increasing probability of positive events (opportunities) and diminishing the probability of negative events (threats). This will determine the success of our projects, or simply, the prevention of attacks, failures, disorders… in our business processes.

In order to provide the right resources and time to perform risk management, it is necessary to plan it, from the methodology, to budget, timing, risk categories identified, responsibilities, reporting…

Risk management follows a lifecycle that can determine the methodology of our SoD projects. As lifecycles, risk management tasks are continuous and repetitive, since risks evolve and are shown in different shapes along the way. It is impossible to build the perfect model of risk that eliminates every potential risk because there are always unknown risks that we cannot identify or control. For these unknown risks, it is recommendable to dedicate a contingency reserve, i.e. an amount of money from our retained earnings that covers unforeseen losses in our business.

5.2 Risk Identification

The first step from this lifecycle is to recognize potential risks of fraud that can affect our enterprise and are inherent to our business processes.

There are risks which are known by the enterprise and others that are unknown.

In the first category, there are direct risks if they are under our control (e.g. SoD conflicts); or indirect risks, if they are not under the enterprise control (e.g. cyberattacks).

The second category, unknown risks are those mentioned above, for which the enterprise will dedicate a contingency reserve.

Firstly, by identifying **sensitive transactions**, we can comprehend those business processes that are more critical in our company, thus, should be closely watched. In addition, there must be determined the SoD conflicts existent in the company. These will be determined through the definition of the functional and technical matrixes (section 5.1.1. and 5.1.2).

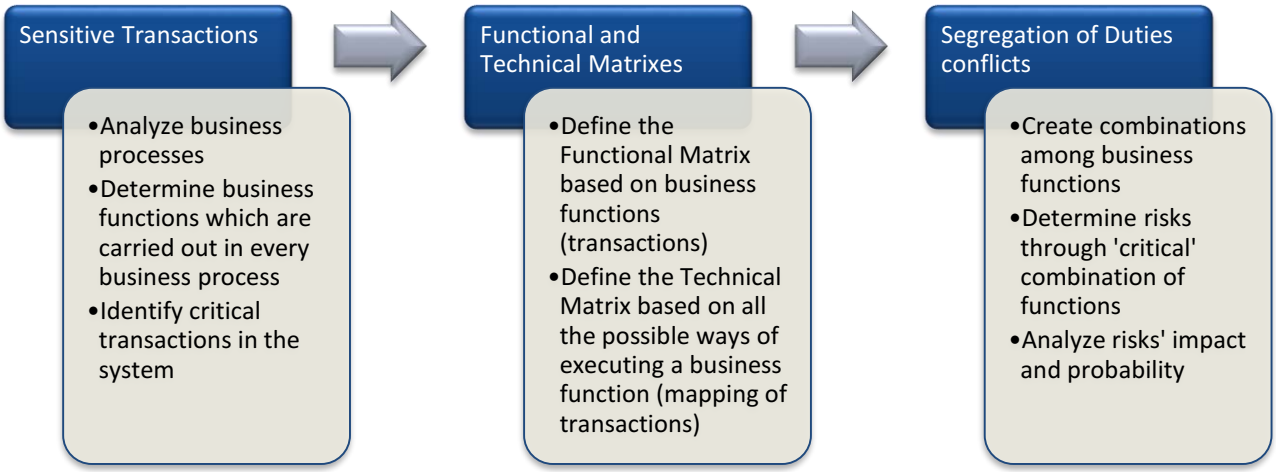


Figure 24: *Risk Identification Process. Source: Own elaboration.*

In addition to these critical system elements, the company must identify the employees and departments that due to its operability are more prone to commit each of the identified **risks of fraud**, and discover the methods that can be used more likely by fraudsters.

5.2.1 Functional Matrix Definition

In order to define a functional matrix that fulfill correctly segregation of duties, these are the steps to follow:

1. **Definition of the functions** that correspond to different business processes that have been identified in the enterprise, such as fixed assets, treasury, procurement…

   The list of these functions will depend significantly on the company and the business processes that are run internally. Some examples of business processes are Fixed Assets, Accounting, Financing, Taxes, Payments, Treasury, Material Management…. These business processes usually correspond to ERP Modules such as Controlling (CO), Plant Maintenance (PM), Financial Accounting (FI), Sales Distribution (SD)…
   See Section 2.2.2 for more information about SAP Modules.

2. Thorough study of the functions performed by each group of people in a department with access to the system (SAP or any other system). Through this research, the enterprise must define a clear and up-to-date **matrix of all functions**.
   See Appendix B for more information about the main functions in the Controlling module, which are obtained from analyzing the business workflow related to it.

This functional matrix is not industry standard, since job positions are different in every company, so it depends on its size and the industry; in addition, functions and names may vary.

By way of example, a functional matrix has been designed with three different functions related to diverse business processes: Fixed Assets, Treasury and Purchases.

- Function 1 (Fixed Assets): Divestment of Fixed Assets
- Function 2 (Treasury): Collection Management
- Function 3 (Purchases): Release purchase order

	Function 1.	*Function 2.*	*Function 3.*
Function 1.			
Function 2.			
Function 3.			

Table 10: *Example of a functional matrix. Source: Own elaboration.*

	No SoD conflicts
	SoD conflict detected
	No conflicts among the same function
	Fields not evaluated

Table 11: *Legend of colors of a functional matrix. Source: Own elaboration.*

Below the gray marks, there are the same crossings of functions than above these marks, so the bottom area is not evaluated, but the upper area.

The SoD conflict found by the crossing of Function 1 and Function 2 is referred to the risk of fraud that can be carried out if a user with access to both functions can process invoices by divestment of assets to customers for a lower value and then record its collection (in collusion with the customer in exchange for favors / commissions).

5.2.2 Technical Matrix Definition

A technical matrix is the deployment of the functional matrix from the perspective of authorizations. In order to build a technical matrix, the enterprise should do a previous analysis of definition of roles or profiles in the security system of the company. In case of inexistence, the enterprise must define the relationship between roles/profiles and functions performed in the system.

The technical matrix is totally dependent on the security system implemented in an ERP or any other management enterprise security tool.

In order to define a technical matrix that fulfill correctly segregation of duties, these are the steps to follow:

1. **Identification of the transactions** that represent accurately the operations of each of the functions included in the functional matrix for SoD.

   Every department or business area should provide a list of the transactions codes used for each of the operations that they execute. Once this list has been provided, we would need to analyze a description of the transaction. In a SAP scenario, the table TSTC lists all transactions implemented in the system along with their descriptions.

2. **Identification of the authorization objects, fields and values** required to be set up in order to execute a transaction.

In order to obtain the parameters needed to execute a transaction, there are some transactions in a SAP scenario that can help us.

The transaction SU24 provides the authorization objects, fields and values that are reported and documented in SAP which are being checked by the system, through AUTHORITY-CHECKs when being executed its transaction source code.

In case this transaction was not well documented in SU24, another solution would be tracing the transaction, so analyze every authorization object with its corresponding values that are actually checked by the system. In the transaction ST01 enabled for traces, there will be a list of authorization objects identified and required to execute completely this transaction with the necessary privileges.

3. **Mapping of transactions.** A SoD process based on risks should ensure that a company figure out every possible method of executing a transaction. Mapping all ways in which a user can execute a transaction is essential for describing a technical matrix adequately.

   It is very common that for a particular business function, users can access to various transactions to carry out this activity. In that case, the security team should verify that the same objects are checked for all these transactions, and users cannot access other transactions or other functionalities not allowed for this user. To do this, these different transactions will have to be configured the same way in the transaction SU24 so that the system checks the same objects.

   By contrast, sometimes transactions have been programmed differently among them and check some objects not permitted because of security reasons, such as jump queries to unauthorized transactions, enabling functionalities that can encourage fraud, capability to perform other different business functions to the transaction involved… In this scenario, the security team should ask developers to change the program of this transaction in the system so that it meets the security rules that have been considered.

hh:mm:ss:ms	Tipo	Dura (us)	Objeto	Texto
09:08:48,186	AUT.		S_TCODE RC=0	tcode=FB01;TCD=FB01;
09:08:48,189	AUT.		F_BKPF_BUK RC=0	tcode=FB01;ACTVT=01;BUKRS= ;

hh:mm:ss:ms	Tipo	Dura (us)	Objeto	Texto
09:09:04,949	AUT.		F_BKPF_BUK RC=0	ACTVT=01;BUKRS=BOES;
09:09:04,959	AUT.		F_BKPF_KOA RC=0	ACTVT=01;KOART=K;

Figure 26: *Trace ST01 of transaction FB01 in SAP. Source: Own elaboration.*

The transaction ST01 lists authorization objects that are checked by the system. Then, the complete list of the authorization objects checked are included in a list of transactions documented. In this list, there are the transaction code, the environment, authorization object, authorization field and range of values.

Once the list of transactions in which a function can be executed, we can build the technical matrix.

ACTIONS	VSYSKEY	AUTHTREE	FROMVAL	TOV
FB01	EPC	F_BKPF_BED||ACTVT		
FB01	EPC	F_BKPF_BED||BRGRU		
FB01	EPC	F_BKPF_BEK||ACTVT		
FB01	EPC	F_BKPF_BEK||BRGRU		
FB01	EPC	F_BKPF_BES||ACTVT	01	01
FB01	EPC	F_BKPF_BES||BRGRU		
FB01	EPC	F_BKPF_BLA||ACTVT		
FB01	EPC	F_BKPF_BLA||BRGRU		
FB01	EPC	F_BKPF_BUK||ACTVT	01	01
FB01	EPC	F_BKPF_BUK||BUKRS	$BUKRS	
FB01	EPC	F_BKPF_GSB||ACTVT		
FB01	EPC	F_BKPF_GSB||GSBER	$GSBER	
FB01	EPC	F_BKPF_KOA||ACTVT	01	01
FB01	EPC	F_BKPF_KOA||KOART	K	K

Figure 25: *Transaction FB01 documented (System, Authorization Object, values). Source: Own elaboration.*

The technical matrix is formed by all the possible ways that from different applications we can execute the same transaction, i.e. there may be 20 ways in an application of making a payment to a supplier. Usually the company only know and use 5 of them, but the security department finds other 15 ways of accomplishing this task. In the system, only 5 of these ways are restricted and controlled, but the others are not under the company control. These have to be analyzed and taken into consideration for the technical matrix design.

A frequent enterprise failure is to map only those transactions that are executed. This would be a scenario as the mentioned earlier. There may be transactions in menus that are assigned through roles, that users do not execute but have access to them. These transactions need to be controlled and taken into account for its analysis

	Application 1	*Application 2*	*Application 3*
Function 1	2	4	0
Function 2	0	2	3
Function 3	0	0	0

No. of privileges (access methods) mapped

Table 12: *Example of a Technical Matrix. Source: Own elaboration.*

In the example above, there are three functions represented, however, a real technical matrix should include all functions executed by the enterprise.

- Function 1 (Fixed Assets): Divestment of Fixed Assets
- Function 2 (Treasury): Collection Management
- Function 3 (Purchases): Release purchase order

Additionally, there are three applications represented, however, a real technical matrix should include all applications that an enterprise use.

- Application 1: IQMS Financial Management: Fixed Assets Module
- Application 2: SAP ERP: FI & FSCM Modules
- Application 3: Microsoft Dymanics NAV

Application 1, IQMS where the company has the Fixed Assets Module, is specialized in how to manage assets' financial and tax reporting. Collection management will be carried out from this application.

In the application 2, SAP ERP, there are two modules running: FI and FSCM. From this application, we can accomplish different functions: function 1 (FI) and function 2 (FSCM), but there is not available any software to manage purchasing processes.

In the example shown, Application 3, Microsoft Dymanics NAV and its ERP management program for Central purchasing. In this application, there are three ways of releasing purchase order.

5.3 Risks Analysis & Assessment

In this phase, risks have already been identified and we have under control every transaction (executed or not in the system) that users can access. SoD conflicts have been identified, so risks of fraud have been recognized.

Risks have to be assessed through measuring its probability and impact in the company.

By using a quantitative analysis of risks, the company must assign an economic value to each risk. Risks are assessed depending on its materiality. Materiality is a SoD term referred to how to measure the impact of a risk.

Materiality (EY, 2010) "is the financial threshold or impact a potential SoD conflict can have over a company's financial statements."

Based on the materiality of risk, the enterprise has to assess which is the financial threshold in order to compare risks with each other.

Those risks with higher economic values are those that can result in fraud or failures in the company, and therefore those to which the enterprise should respond.

The enterprise should also consider the probability of the identified risks. For example, risks with a very high economic value but a very low probability will be controversial. Companies should consider if it is effective or not to implement a plan to avoid them. This decision will depend on the company preferences and its resources (time, money...)

On one hand, the enterprise will **accept and document those risks** with low probability and a low materiality. On the other hand, the company will dedicate a **contingency reserve** for risks with high impact but quite improbable to occur.

Risks to which the company will prepare an action plan are those with high probability and high impact, thus, a high economic value (high materiality).

5.4 Action Plan

In the action plan phase, it is when the company has to find a strategy to respond those risks with high impact and high probability. Those risks, as result of SoD conflicts, are being analyzed and controlled.

In this phase, the company has to define measures and response to risks. The objective is to develop and analyze different **responses to risks**, take decisions about what actions to implement in the next phase and assign responsibilities when risk management. It is also significant planning the action to carry out such as setting deadlines, budgets…

From a risk management approach, when we face a fraud risk in a business process, the enterprise can perform different types or responses:

- **Accept**: this is the typical response that companies used to carry out, not implementing any plan to prevent it, simply, accept its occurrence.
- **Avoid**: when a company finds risks in particular countries or markets, and the way to solve it is not entering in that market or not expanding to a specific country because of the risks it involves.
- **Transfer**: when a company hires an outsourcing firm and transfer that risk to it, since they know better how to manage risks and control them.

- **Control**: fraud risks have to be controlled, offering solutions where risks are monitored and managed under the company's boundaries
- **Mitigate**: risks can be reduced to its minimum level till being totally eliminated when controls are well performed, thus, risks become minimal and barely exist.

The solution to prevent fraud risks is to search and establish **preventive controls**. Such anti-fraud controls will reduce and mitigate the risks identified.

5.4.1 Stakeholders in decision-making

In the action plan, IT and finance areas are both interested in risk management in order to provide a complete SoD process.

The **finance** area knows the materiality of risk for measuring the impact of every business process and the mitigating controls to provide in every area.

The **IT area** builds on the risks captured by **internal control** and measured by the finance area and enters it into the computer system as authorization data to result in access control remediation.

All this process has to be go hand in hand with **top management** as they have a general overview of the operations of the company and recognize more precisely the importance of each of the risks based on available resources and weaknesses of the company.

5.4.2 Mitigating Matrix Definition

The solution to mitigate risks is by building controls that reduce the impact of such SoD conflicts, almost to its complete reduction.

In order to define a mitigating matrix, there are some steps that should be followed:

1. Thorough study of the combination of functions and analysis of **risks intra-process** (within each process), inter-process (with other processes) and critical action.

2. Once defined corporate risk matrix (Functional Matrix) from internal control matrixes, the **mitigating controls** that can be applied to these risks defined for each particular case are identified.

Continuing the above example, the SoD conflict identified by the combination of Function 1 and Function 2 was related to the risk of fraud that can be carried out if a user with access to both functions can process invoices by divestment of assets to clients for a lower value and then record its collection (in collusion with the client in exchange for favors / commissions).

As a mitigating controls, the enterprise could establish that:

- All invoices entered either from the Logistics module or from the FI module remain locked until they are released for payment according to the authorization matrix.
- Thorough review of clients and support related to invoices
- Review of the counterpart to the disposal of assets for a lower value
- Review of unbilled receipts of good or commissions
- Check SoD rules related to Access Control in order to monitor access to these specific functions

	Function 1.	*Function 2.*	*Function 3.*
Function 1.			
Function 2.			
Function 3.			

Table 13: *Example of a mitigating matrix. Source: Own elaboration.*

	No SoD conflict
	SoD conflict mitigated
	No conflicts among the same function

Table 14: *Legend of colors of a mitigating matrix. Source: Own elaboration.*

After this analysis, there must be an evaluation of the current SoD conflicts in order to be reduced to its minimum level. The mitigated SoD conflicts will be highlighted with yellow marks and will deploy its mitigating controls. In this process, the company can start enforcing least privileges for users and restricting them access only to their job responsibilities.

When establishing mitigating controls, it can be assigned a **mitigation monitor** that is the individual that will check if the mitigation has been performed correctly. In the mitigation control tab, **alerts** can be set through an alert generator when risks are committed or when attempting to carry out a SoD violation.

A **mitigation approver** is assigned to controls and is responsible for approving any change to the controls defined.

5.5 Implementing Solutions

In this phase, the enterprise has to implement all the measures mentioned in the previous phase.

Mitigating controls take place following the solutions planned when changing SoD conflicts to a mitigated SoD conflict in the matrixes seen previously.

In the implementation phase, not only mitigation controls are considered, but also the implementation of rules that will let us provide measures to prevent SoD violations. In order to achieve this automatic set of rules, a company has to implement a rule set of every information captured in the preceding phases.

A SoD rule set has to be customized for a specific firm, since every company has different business processes, thus, it can be affected by different types of risks.

In order to automatize these controls and violation checks, the company will ensure that in its ERP or any other tool used to manage its business process there is a functionality to enable these rules.

In scenarios such as SAP, there are **default rule sets** configured with the standard SAP transactions and most used business processes. However, if used this default rule set, the company will need to add custom transactions, or authorization checks which are not SAP standard. In addition, in the default rule set, there may be risks that are not applicable to our company, so such risks will be disabled. After this revision, the company should add to these risks those that have been detected from SoD conflicts and fit our business processes.

The format or structure of this rule set will highly depend on the application used. In a SAP scenario, a rule set is a spreadsheet file that is imported to SAP GRC to analyze the SoD implemented and make it life in the SAP system.

In this spreadsheet, there are several tabs:

1. bp – list of codes of all the **business processes and their description** (e.g. FFAA Fixed Assets)
2. funct – list of codes of all **functions and their description** (e.g. AF01UX0 AF01 – Registration of immobilized suppliers' invoices)
3. functact – combination of a **function with the transaction** codes where this function can be developed – all the methods where this function can be executed – (e.g. AF01UX0: transactions AB01, AB02, AB08, ABGF, ABGL…) Every transaction is in a separate row related to its function.

4. functbp – combination of **functions and business processes** codes (e.g. AF01UX0 FFAA)
5. risk **– risks resulted from SoD conflicts**: combination of functions, 1st value is the risk code, then the two functions that conflict and a risk category code (e.g. FI088UX0: AF01UX0 CA01UA0 FINZ) Based on the Functional Matrix Definition.
6. riskdescr – list of **risks and their description** (e.g. FI088UX0 AF01- Registration of immobilized suppliers' invoices & CA01A – Management of FI accounting periods)
7. rrsr – lists of **risks codes associated to the client** where they run (e.g. FI088UX0 SANDRA&CO)
8. ruleset – list of **client rule set name** and its description (e.g. SANDRA&CO Rule set designed for Sandra Morillejo Thesis)
9. funcperm – list of functions related to the **transactions** where this function can be executed and the **authorization objects** that are being checked in order to have access to them. It is based on the Technical Matrix definition. The table below shows a brief summary of the information in this tab.

Function Code	Transaction Code	Auth. Object	Auth. Field	Auth. Value (Range start)	Auth. Value (Range end)	Logic operation for auth. values
AF01UX0	AB01	A_B_ANLKL	ACTVT	01	01	AND
AF01UX0	AB01	A_B_ANLKL	ANLKL	ZXXX	ZXXX	AND

Table 15: *Example of Rule set funcperm tab (based on the Technical Matrix Definition). Source: Own elaboration.*

Besides all technical implementations such as mitigating controls and the definition of a rule set, the mission of a corporate governance is to define an anti-fraud culture to prevent any risk (a zero tolerance culture). This type of prevention policy should involve from top management to the last employee incorporated thereto.

The antifraud culture should follow the recommendations featured in section 3.1.2. Some of these anti-fraud measures could be to review and improve internal controls and **anti-fraud programs** in key departments, reformulating **variable compensation** programs, providing training for staff on the regulatory framework applicable to anticorruption international standards and business ethics, implementing a complaints channel or **ethical line** and complaints procedures, and so on.

Another anti-fraud control could be **monitoring suspicious transactions**. Critical transactions could be traced and reported so managers or the IT team can check if these

operations meet the standards reliably. In order to monitor these transactions, the company has to define rules where these critical transactions or functions are monitored in the configuration parameters related to Access Control.

5.6 Measure, control and monitor risks

The last step consists of the evaluation of controls and processes that ensure that identified risks have been analyzed, mitigated and implemented in an efficient way.

The objective is to perform **control and monitoring** tasks of the resulting risks following the implementation of mitigation measures.

Some of the steps to be followed are:

1. Identification and **assessment of residual fraud risks** arising from the absence of controls or ineffective controls.
2. Response to residual fraud risk

All these steps determine and close the risk management lifecycle, but as mentioned, this is a continuous process, not a project that ends once a response to risks is implemented. Segregation of Duties has to be understood as a process, since the company evolves, as well as risks that can impact our company.

6 METHODOLOGY OF A SOD PROJECT USING SAP GRC ACCESS CONTROL

An enterprise that needs to implement segregation of duties bearing in mind risks, corporate governance and compliance can use the powerful tool SAP GRC Access Control to achieve it.

SAP methodology for projects is based on delivering value and adapt to changes from an agile approach. Companies need to respond quickly to risks and changes in both the internal and external environments to create solutions in an efficient and flexible way. This the reason why companies have changed from traditional waterfall methodologies to agile methodologies. SAP developed its own methodology: ASAP, which lifecycle is based on Scrum and Lean, which are based in:

1. Agile risk identification and management
2. Implementation of operative functionalities structured in short development cycles (sprints), starting with those with higher priority, thus, those that bring more value to the client
3. Fast information retrievals and value earning
4. Continuous participation in the project
5. Increased flexibility in implementation
6. Improved control and monitoring of the project

ASAP methodology is designed for implementing a SAP project from scratch. In this case, ASAP is not applicable since our approach is building a SoD model by using the tools provided by SAP GRC Access Control in a SAP environment already implemented or other non-SAP application. However, this type of projects is agile too. When SAP GRC AC is implemented in a company, it increases largely the speed of fulfilling access requests, provides control in every critical situation, access controls are reviewed, consistent and automatized, resources are shared easily and accessed when needed…

The phases followed in this project were the following:

1. An exhaustive **analysis of SoD** to identify SoD risks, recognize business processes and tasks, identify every critical element in the system to control it, group users by function or job position, and so on.
2. A **design** phase where the role security model is developed taking into account the business functions identified to comply with SoD
3. The **implementation** step is where the role model is analyzed to ensure there are not SoD conflicts in the roles designed, then rules take shape and, if any, corrective actions are performed and reported.

4. In the **testing** phase, roles assignations are tested in the Quality environment, so users can check if they have privileges only for the tasks they are supposed to perform according to their job positions.
5. The last phase is **maintenance**. This phase is endless, since as we mentioned, SoD is not a project by itself but a process. Company's departments will change, new business areas will be created, new transactions in the system will be developed, new users and job positions will be created… This phase is where the model is already implemented, but it must be subject to change at any time to meet the business needs.

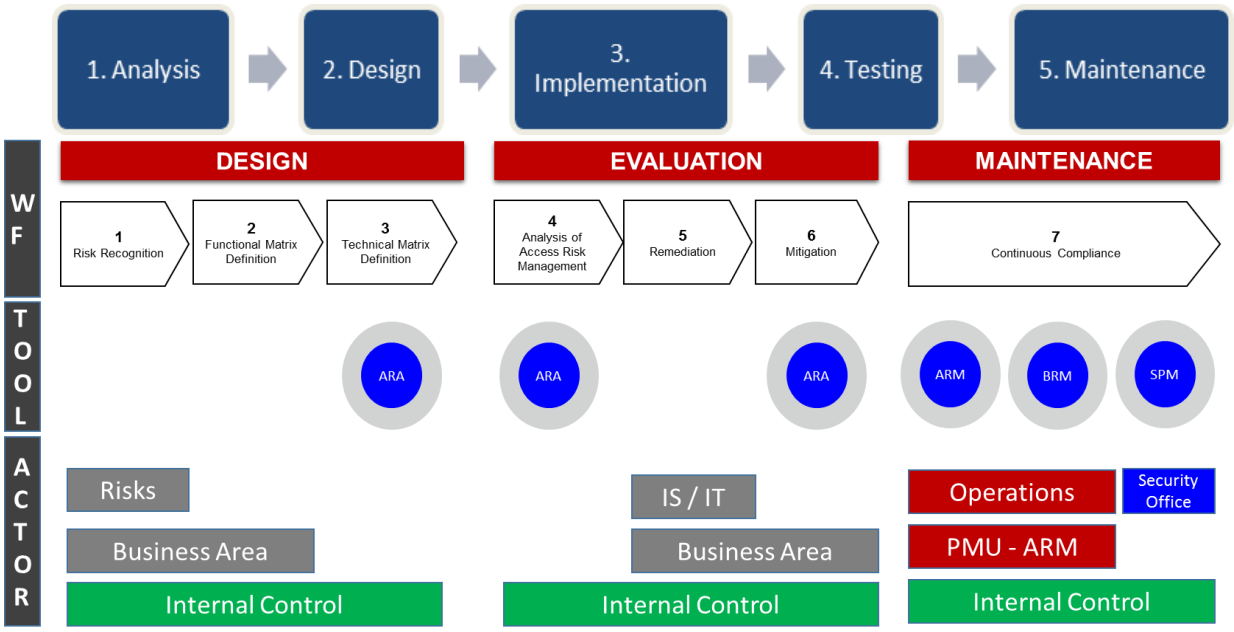


Figure 27: *SoD Project Phases where different actors are involved using SAP GRC Access Control tools. Source: Own elaboration.*

There are the main functionalities that SAP GRC Access Control tools offer in each of the project phases:

- AMR (Access and Manage Risks) or ARA (Access Risk Analysis) will be used after Functional Technical Matrix Definition in order to analyze the risks identified and monitor them, as well as creating alerts to prevent risks in all business processes.
- BRM (Business Role Management) enables to create roles, implement authorizations and maintain roles over time. It enables role provisions to users
- ARM (Access Request Management) is used in the maintenance phase. It is a tool to support user incidences related to SAP access, such as requesting new transactions or roles. This tool includes an approval workflow.

- EAM (Emergency Access Management) or SPM (Super-user Privilege Management) will be used by users to access critical tasks in emergency situations. All the actions performed by this super-user access will be controlled.

6.1.1 Overview of the most critical transactions and tables in SAP

There are some transaction codes that are going to be useful when implementing SAP GRC Access Control as well as a streamlined SAP security configuration.

See more about transaction codes or T-codes in the Background and Preliminary Concepts section.

In the table below, there are represented some T-codes and its description, along with their main functionalities.

T-code	Description	Functionality
SU24	Maintain Authorization Defaults	- Display and update the values in tables USOBT_C and USOBX_C - Restrict access to transactions based on the authorization objects checked - Add or subtract the checks performed in the transaction by changing the appropriate flag
ST01	System Trace	- Execute transaction trace - Display all checked authorization objects, the values assigned over the check and objects which may lead to a missing authorization behavior
SU53	Evaluate Authorization Check	- Display the missing authorization object that a user is not assigned in its roles/profiles to access a particular transaction or function within a transaction.
SE16	Data Browser	- Display information from SAP tables
SE11	ABAP Dictionary Maintenance	- Display information from SAP tables, and also their structure - Create, change and display table entries
SM30	Call View Maintenance	- Access to tables with a maintenance dialog defined - Critical transaction for all the functions that can be enabled in every table
SE30	ABAP Runtime Analysis	- Execute performance or flow analysis of an ABAP program. - Measure performance and find bottlenecks
SA38	ABAP Reporting	- HIGHLY critical (access not given to any user in the Production Environment)

		- Run directly programs or reports in SAP
SM49	Execute external OS commands	- Execute external operating system commands in SAP GUI
SM59	RFC Destinations (Display/Maintain)	- Configure and display RFC Destination
SP01	Output Controller	- Maintain the spools: delete, print, save local files... - Spool administration
SP02	Display Spool Requests	- Display and monitor spool requests
SE01	Transport Organizer (Extended)	- Change and transport organizer - Create, change, view logs, display transports (all tasks related to transport requests)
SE09	Transport Organizer	- Workbench transport requests - Release transport orders - Track changes to ABAP workbench objects (dictionary, reports, pools…)
STMS	Transport Management System	- Import transport order from the source environment to the destination system
SM01	Lock Transactions	- Lock or unlock instantly transaction codes in the system, so any user can access it

Table 16: *List of T-codes (SAP transaction codes) which are critical in SAP security configuration in a SoD project. Source: Own elaboration.*

In the table below, there are represented some tables and its description, along with their main functionalities, that are useful to determine certain information when managing roles and transactions in SAP.

Table	Description	Functionality
TSTC	SAP Transaction Codes	- Display all transactions implemented in the system along with their descriptions, programs associated…
AGR_TCODES	Assignment of roles to Tcodes	- Display the roles where a particular transaction has been assigned (included in its intrinsic profile)
AGR_USERS	Assignment of roles to users	- Display all the roles that are assigned to a specific user
USOBT_C, USOBX_C	Maintain Check Indicators	- Display the relationship between a transaction and its authorization objects - Store check indicators maintained in SU24

Table 17: *List of tables which are critical in SAP security configuration in a SoD project. Source: Own elaboration.*

6.2 Analysis of SoD

The analysis of Segregation of Duties in a SAP system is a complex task since there are many factors and settings to take into account before building a complete and secure SoD model.

As was mentioned in the section 5, it is important to look at SoD from a risk perspective.

Firstly, we should identify risks resulted from SoD conflicts when defining the Functional Matrix. Then, analyze all the possible ways of performing a specific function in the system, i.e. from all the applications that the company uses for business processes.

When identifying all the critical functions in conflict, the enterprise should identify the elements that are most critical to segregate correctly these tasks. Such elements are transactions and authorization objects which are quite critical in the system, not only because of combination with other critical functions, but because the intrinsic risk containing in themselves.

6.2.1 Identification of Critical Processes and Sensitive Transactions

Firstly, it is important to identify **critical processes** as well as SAP standard transactions that execute those business processes.

Consultants have to take into consideration the most critical transactions when building roles. In SoD terms, these are known as **sensitive transactions**.

Sensitive transactions are those labelled as highly risky when implementing the functional matrix which supports the foundation of a proper **segregation of duties**.

In addition to these critical functions, there are critical transactions in SAP whose access should be limited due to the security risks that imply. Some examples are SE11, SE16, SE30, SA38, SM30, SE16M, SM49 (creation of system orders) and SM59 (execution of system orders). The use of these transaction with inadequate access may pose a risk to the company data since a lot of tables can be altered (SE16/SE16M), external OS commands can be executed, any SAP program can be run (SA38), and so on.

Depending on the company security decisions, some of these transactions will be limited to only few users for specific reasons, and other transactions will be directly prohibited for all users in the system.

6.2.1.1 Transactions Z or Y**

There are also some transactions that are developed exclusively for the company, customized for its business needs. These transactions usually start with Z or Y. These type of transactions must be checked by security consultants since they have not been programmed or validated by a technical SAP support team, but by an external software developing team.

6.2.2 Identification of critical authorization objects

Secondly, SAP consultants need to determine the **authorizations objects** required for these transactions. In addition, the authorizations that are critical in SAP over these objects should be customized into SoD rules in order to avoid the generation of false positives, and negative false.

Before building roles, we should consider which are the most **critical authorization objects** that users need to access to perform their duties. This is a list of the authorization objects that deal with System Administration (thus, start with S) whose access should be restricted or forbidden:

7. Security for tables: S_TABU_DIS (authorization group for a table), S_TABU_NAM (name of the table) and S_TABU_CLI (for client independent tables).
8. Reports or executable programs: These are protected by S_PROGRAM, which checks it the user executing a program is included in the group authorized for it.
9. Files from programs: S_DATASET provides access to the specified filename in the OS of the program that is being run. Using this object, it can be determined the activity permitted: read, write, deletion…
10. Spools: A spool is a recipient of print requests which provides a number of utilities for controlling the output of information storage. Many objects give access to spools: S_ADMI_FCD, S_SPO_ACT, S_SPO_DEV and S_SPO_PAGE.
11. Users / Roles: Using objects that control user administration, different roles can be created to segregate these functions. S_USER_AGR, S_USER_GRP, S_USER_PRO and S_USER_AUT are some examples.
12. BDC (Batch Data Communication) sessions: S_BTCH_ADM, S_BTCH_JOB, S_BTCH_NAM are the objects that determine the activities authorized when loading data into SAP (batch sessions). The automatic background process that enters data into a transaction is defined as batch input. Every batch input executed in SAP is recorded in the SM35 transaction.
13. ABAP Workbench: S_DEVELOP is the authorization object that controls ABAP development objects. These controls include object type, object name, activity…

All these security controls must be set up in order to achieve a safe and complete architecture that controls all critical elements such as activities, transactions and authorization objects.

6.2.3 Identification of Enterprise Structural Elements

Some elements related to the structure of the organization should be defined prior the construction of a SoD model.

1. Consultants should map the **organizational values** of the company: organizational codes, cost centers, purchasing groups…
2. **Business processes** and application controls associated to them. If the company processes are not aligned with a common and integrated model, changes to business processes will be required.
3. Users should **be grouped by similar tasks** or activities carried out along business processes. Simultaneously, users could be also gathered together by geographical location. These user groups need to be approved by the corresponding **business area leader**.

6.2.4 Identification of Transactions for the Functional Matrix Definition

After having identified critical transactions, critical authorization objects and enterprise elements, such as all the business processes, SoD analysts have to recognize the inter-process and intra-process risks affecting the company. Therefore, the tools used will be those that extract risks from SoD conflicts: functional matrix, technical matrix and other mapping techniques transactions. See more about this whole process in sections 5.1.1 and 5.1.2.

Firstly, SoD analysts have to consider which are the transactions that are been used by users in the systems. A technique could be monitoring the transactions used for a period of time. Another technique (and quite used) is to obtain the statistics from the system of the transactions that users have been using for a certain period of time. This information can be queried through SAP transaction SE16 and with help of the tables AGR_TCODES and AGR_USERS to be able to identify who uses what.

In this redesign model, SoD analysts have to make a list of the transactions executed and not executed by users and transactions that have been executed by a functional business area and not executed by a business area.

Based on this list, we can build the functional matrix and seek for crossings of risks (SoD conflicts).

Human Resources will provide SoD analysts a list of current users in the system and an updated organigram of business areas in the organization. Every department manager will provide SoD analysts what tasks should be performed in the system (not what they are currently performing, because these operations may vary with a correct SoD analysis). It is important to exactly know:

- A clear and streamlined list of tasks and processes that should be carried out by each department in the organization

- A list of users that correspond to every business area, or department and they perform the same tasks, so they will have the same business roles

Once this information is complete, the design phase could start.

6.2.5 Risk monitoring and remediation using SAP AMR

The SAP GRC tool that can help us to automatize this risk identification process is AMR (Analyze & Manage Risks), previously ARA (Access Risk Analysis).

AMR basically consists of a repository of definition of SoD rules and critical transactions. One of its benefits it that it will check the rules established for user activities and for role management tasks and will ensure these do not introduce new risks to our company. In addition, AMR reports a list of the risks existing within the current SAP security configuration and according to the Security role model defined.

AMR inflows:

1. The security model defined of risks created from the combination of functions.
2. Data collected by AMR such as users, profiles, roles, transactions, authorizations…

AMR outflow:

1. AMR processes all incompatible functions in the system to provide a report of the number of risks in the system in categories of highly critic risks, high risks, medium risks and low risks.
2. Provides solutions to prevent these risks through deleting authorizations with conflicts or by implementing mitigating controls to the identified risks.

This risk analysis and remediation tool generates and maintains automatically this process of identifying risks, mitigating conflicts for users and roles, and providing a continuous monitoring of access risks and user roles assignments across the enterprise.

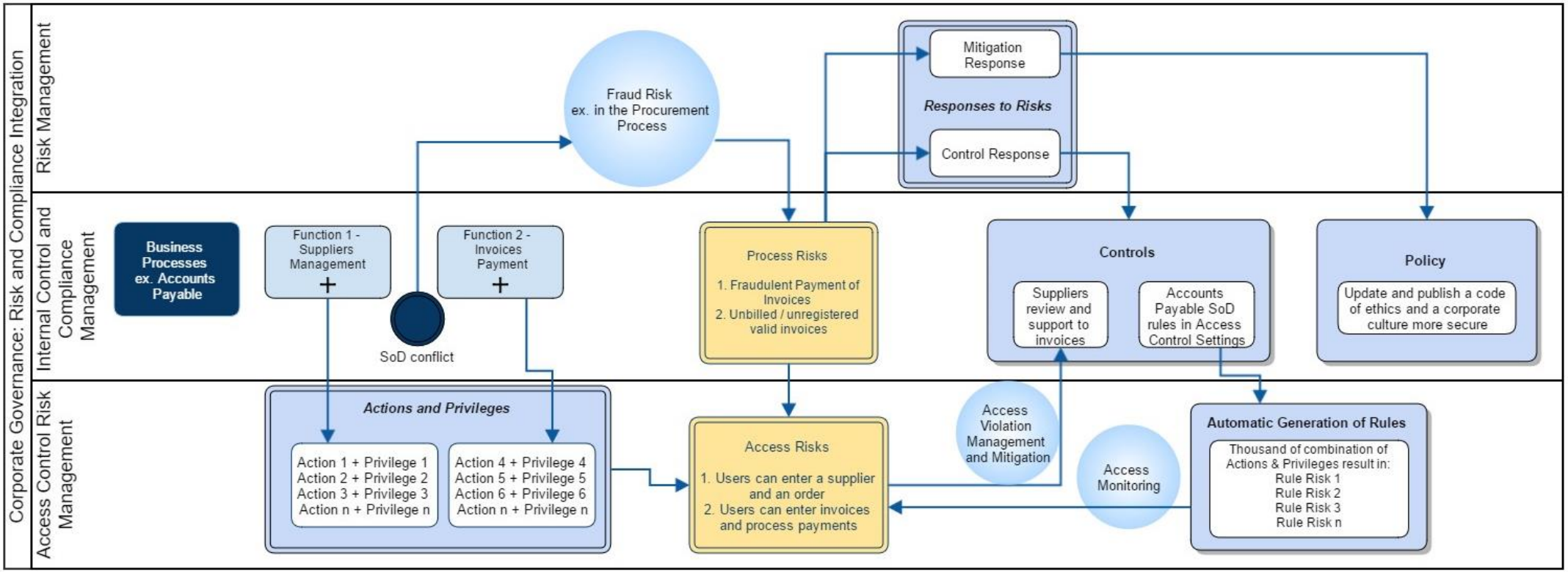
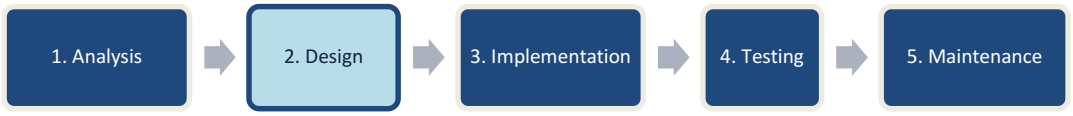


Figure 28: *Corporate Governance: Risk and Compliance Integration. Source: Own elaboration.*

The figure above represents how different GRC teams are involved in the SoD project and Access Control architecture. This diagram shows from the business process identification to the different rules and controls that are applied automatically by using SAP GRC AC ARA. This is how SoD is structured from a risk-based approach in an enterprise system. IT Security Management, Internal Control and Compliance and Risk Management have to collaborate together to make this process live, in an integrated and cohesive way.



6.3 Design

Once the functional and technical matrixes have been designed and risks have been identified, it is important to design and build a security model that ensures segregation of duties.

The definition of this new model of authorizations has to be based in the functions performed within the business. This model has to offer flexibility and modularity, so it is possible to make future changes and maintain it in a clean and agile way. New roles can only provide privileges to the required functions determined by job position.

6.3.1 Critical Activities: Read-only access vs Read-write access privileges for the Authorization System Model

When constructing the authorization architecture based on **roles and profiles**, there will be roles that contain certain functionalities which are more simple such as access to print accounting documents, or access to read/view sales reports. These roles will be less critical in the system since these access permissions do not create or change any document in the system. Clients can set if display access is critical for them, but it is not usually the case.

However, security consultants must pay attention when creating roles for more **critical activities** such as creating, changing accounting documents, releasing, deleting or removing them. These type of activities is critical in the system so it is important that the role that contains them is only assigned to users in charge of these activities, such as the accounting department, but not to any user.

6.3.2 RBAC – Building a Role Based Access Control Architecture

As has been disclosed throughout this document, the security architecture that implements more easily SoD is a RBAC (Role-based Access Control) approach.

For building roles in the system, we have to distinguish among single roles, composite roles and business roles.

See more about what a role is, single roles and composite roles in section 6.2.1 Roles. See more about how to create single and composite roles in SAP in the Appendix A.

In a SoD model, there can be built different roles. It depends on the organization preference or the SoD consultant design. In the design explained below there are five different type of roles designed: Environmental Roles, Functional Roles, Composite or Job Position Roles, Organizational Roles and Business Roles.

In the category of single roles, there are defined different subcategories: Functional roles and Organizational roles.

1. **Environmental Roles** are single roles that are assigned to all users in the system. It is a basis role that include all transactions or common tools to all users as managing spool (SP01, SP02), managing user preferences, error handling, etc.
2. **Functional Roles** are single roles that include transactions that allow to execute a certain function, as well as authorization objects necessary for its implementation However, there cannot be authorized any authorization object related to organizational values. These roles must be absolutely independent of any organizational values so they can be used transversely for any of the firm subsidiaries, cost centers, etc.
   Functional roles need to be differentiated into two types for visualization tasks and for change or update tasks. In this way, there are:
   - Read-only access privileges: Users are authorized only for visualization. This access scope is associated to activities 03, 08, 09, etc.
   - Read-write access privileges: Users are authorized also for changes, updates or releasing tasks. This access scope is associated to activities 01, 02, 05, 06, etc.
3. **Composite roles or Job position roles** are those roles compounded with the grouping of functional roles that make up a job position within the company. Composite roles do not include Organizational Scoped Roles since these scoped roles are associated with users and not with job positions. For example, in the CO module, Cost Center Management, Primary Cost Elements Management. See examples of Composite Roles for the CO module in the Appendix B.

4. **Organizational Scoped Roles** are single roles that define the organizational work environment of a user, but does not include privileges to perform any functionality (i.e., they do not include transactions). In this role, all the authorization objects related to organization values are included. These organizational objects are necessary for the execution of a function or different functions included in a job position (defined in a composite role).

Accordingly, there must be distinguished two different type of organizational scoped roles:

- **Function-Scope Roles:** These organizational roles are defined to complement a function with organizational values. That is, these roles are associated with a single functional role.
- **Position-Scope Roles:** These organizational roles are defined to complement a position organizationally. That is, these roles are associated with a position role, or composite role.

Depending on the module, some area-function roles, area-position roles or both have been defined. In case of CO module defined in the Appendix B, the definition of access at the organizational level has been implemented using position-scope roles.

As in functional roles, it is necessary to maintain distinct roles for the display scope and updating scope.

5. **Business Roles:** These roles consist of a set of composite roles and organizational-scoped roles that make up a profile or position within the organization. This business role is assigned to users who perform the same activity within the organization.

These roles have to be named according to the nomenclature defined by the company.

The **nomenclature** proposed in this document is:

Z + Role Type + Module + Organization + '_' + Description + '_' + Suffix

Z: According to SAP note 20643, every new implementation has to start with 'Z', and in default, starting with 'Y'.

Role type: Single role ('<'), Composite role ('<<')

Module: 1 or 2 digits for the module name to which this role functionality is associated

Organization: 2 digits for the organization code, if applicable. XX is the solution when organization is not applicable, in case of functional or composite roles.

Description: Short role description. It will start with U if the role allows Updates or modifications, and V if the role is configured for Visualization. Its length depends on the other values length, but it is not unlimited, since the maximum role length is 30 characters. For word separation, blanks cannot be used, '_' will be the separator.

Suffix: Role ending with 2, 3 or 4 digits that sum up a role description. This suffix will be the same for composite, functional and organizational scoped roles.

1. **Environmental Role:** It is a unique role, it could be named as Z<BXX_USER_GRAL, since it belongs to the Basis Module and is the general user access role that every user has assigned.
2. **Functional Roles.** Ex**.** Z<COXX_UCOST_CENTER_UCOC
3. **Composite roles or Job position roles.** Ex. Z<<COXX_UCOST_CENTER_UCOC
4. **Organizational Scoped Roles** Ex. Z<CO01_**CO0A1H_USCOPE**_UCOC
   The description is split up in 2 parts: the description (ex. cost center code: CO0A1H) + '_' + 'U/V' if the update or visualization task is performed + 'SCOPE'.

6.3.3 Compliant Business Roles & SoD through SAP BRM

Business Roles are managed in SAP GRC BRM (Business Roles Management), previously known as Enterprise Role Management. BRM apply enterprise role nomenclatures to role creation, diminishing management and the risk of SoD violations.

Business roles form a SAP security design based on **job positions**, not specifically in tasks. A task-based role design increases the number of roles per user, since a user has a role for every task executed. In a job based role approach, security is designed based on positions for a group of users. This decrease the number of roles per user, which is more maintainable and secure.

There are not roles for specific employees, every job position is assigned certain business roles. Every time there is a new user in the system, it is assigned determined business roles according to its position. In addition, there are many processes that can be managed by using SAP GRC BRM:

- **Change of job position**. A user is changed to a different job position, so a new set of business roles will be assigned to this user. However, this user is assigned for a short period of time (ex. 2 months) a temporary user with the previous privileges. If the new job position has not been defined in the system, we will contact the SoD analyst.
- **Temporary replacement**. When a user is laid off for a temporary period, the user that replace this user will be assigned its privileges in a temporary user during this time.
- **Role incidence**. A role can be misconfigured and lack of information. In order to make these changes, the role can be modified. This functional role will have to be then approved by the SoD analyst.

- **New function in a job position**. Business role is modified including this new function. These changes will have to be then approved by the SoD analyst.
- **New transaction in the system**. When a new transaction is created in the system, it can be assigned to a functional role, but a new approval workflow will start. It is important that before this transaction is in the system, it has been documented correctly in transaction SU24.
- **Merger or new firm subsidiary**. Single and composite roles are created in the backend and then imported to SAP GRC where the business role will be built.

Despite business roles implement a more effective security structure, single and composite roles can be also created and maintained through SAP BRM.

BRM has to be configured with an Approval Workflow, so any change in the Role Architecture is approved or rejected by the Role Owner, or in its absence, by the Security Leader. Role Owners are usually SoD analysts, and the Security Lead actor could be represented by Internal Control.

BRM Workflow Steps:

1. SoD analysts define the role.
2. System administrators maintain authorizations, synchronizing them with backend systems.
3. System administrators have the possibility to derive the role to others where it can be contained or related.
4. Before approving the changes in the role, there is a risk assessment report when SoD conflicts are found within the role or with the combination of other roles. There can be stablished rules, controls or other solutions to mitigate them.
5. Process Owner or Role Owner has to approve the role or reject it.
    a. If approved:
        i. System administrators have to generate the role in all the environments in backend.
        ii. SoD analyst or Role Designer has to maintain test cases
    b. If rejected:
        i. System Administrators will be notified in SAP Netweaver and they will be in charge of notifying it to users if required.

6.4 Implementation

Once the security model is designed, it is the time to build it in SAP following the methodology explained above and the directions for a secure environment.

The workflow standardized in BRM processes the results of ARM and its Analysis of Risk and Remediation Rules. After this analysis, BRM verifies if there are SoD conflicts at an intra-role level (within a role among transactions or authorization objects) and at an inter-role level (among different roles).

After this analysis, SoD analysts will have to consider any role conflict or user conflict and report them to elaborate corrective actions.

Roles are built following the BRM workflow steps. The next stage is to assign roles to users according to the design stablished. This stage is described as Role provisioning. Roles have to be assigned from a start date to an end date, which can be marked as 31.12.9999 if the position is permanent. In case of temporary roles, the end date will be marked with the specified date when users cannot be authorized to it.

6.5 Testing

Firstly, it is required to have separation of duties not only in the employees of the organization, but the diverse teams responsible for the design, implementation and testing of this security model in the company.

In order to achieve these different functions, there are three different environments where they work.

6.5.1 SAP Deployment Environment

In any software deployment there is a landscape (environment or tier) where software and computer programs run and are deployed. An environment is composed of servers resulting on a layout of servers, or architecture of servers.

In the SAP scenario, there are three different environments:

- **Development environment (DEV)** is where programmers and consultants carry out the customization of the ERP functionalities based on the company's requirements.

  Regarding to security terms, this area is where new transactions such as transactions Z* or Y* are developed, new programs are edited using the ABAP[10] Development WorkBench, user interfaces are designed, roles are created, profiles and authorizations are conformed. Basically it is where changes are originally made. In this environment, there are no users registered in the system, but only the authorizations, transactions, menus, programs, user interfaces…

  Once developers and consultants have programmed and configured all changes in the Development server, they transport this information to the test server (Quality).

- **Quality environment (QAS)** is where the core team members and other staff test the customization of the software designed and programmed.
  In this testing server, testers check the programs before transporting them to the Production server: it is an acceptance or rejection decision.

  In order to check whether a user can access or not to a specific program (transaction), consultants assign this new program (transaction) to users through new or existing profiles, included in roles. That user can check in its Quality SAP logon if he/she has the right credentials for accessing every option or function in a transaction. Users can also request for changes if a transaction has not been developed correctly.

  Apart from user tests, there are also different tests for checking the new program's performance and also its integration with various modules.

- **Production Environment (PRD)**: is where the real-time data of the company is recorded and stored. Every transaction and business process that is performed by end users (client) will be run and go live. Client data such as transactions, programs, interfaces… are in the production environment once it has overcome the previous stages (DEV and QAS), so all changes recorded in the Quality Environment were transported to the Production Environment.

[10] ABAP is the SAP 4th generation programming language which is used to program most of the R/3 products, SAP Business One, etc. This programming language is totally integrated with SAP system, and it is oriented to a sequence of events depending on the compliance of one condition or event.

In order to have real data without misconfigurations in the Production Environment, it is important that every transaction is transported after being tested appropriately in the Quality Environment so we can guarantee the integrity and consistency of the transactions running in PRD.

Figure 29: *Flow of data across different environments. Source: Own elaboration.*

The flow of data is in the direction represented above, but not backwards. The data is transported from one environment to another using transport orders.

Transport orders have to be created including all the new information, changes, new transactions… (Tr. SE01) Once it is created and completed, it is released along with all the tasks included on it (Tr. SE09). After being released, the order has to be imported to the destination system using STMS (Transport Management System).

6.5.2 Security Analysis in the Quality Environment

SAP Security consultants must check that transactions are documented correctly with the right authorizations.

6.5.2.1 Adequate Documentation for Transactions

The steps for analyzing access control for transactions start with the initial execution of the transaction. A transaction must exist, thus, have an **entry in the TSTC table**. Then, the system checks if this transaction has been locked using tr. SM01. In case it has been locked, the execution will be stopped and will not be used by any client.

If the transaction has not been locked and started its execution, as mentioned previously, S_TCODE is the first authorization object that is checked when accessing a transaction. Then, depending on the transaction, a transaction may also require to check other authorization objects.

In the **SU24 transaction**, there is a list of all authorization objects required to access a specific transaction. If the authorization objects for that transaction are checked by the system, users will need to be assigned those authorization objects to access. These objects with the values entered in the tr. SU24 conform the authorizations. These will

be included in a profile, assigned manually to the user or through a role. In this way, users with that role or profile will be able to perform any function in that transaction.

6.5.2.2 User Access denial

If users are not able to access some functionalities in a transaction that is tested on the Quality environment, this transaction will be required to be traced. This process starts when IT Consultants receive a ticket because of the missing authorization.

In the scenario of access denial, there can be some reasons for the lack of access:

- The role did not include the appropriate authorization objects, however, these were checked by the system since they were reported in the SU24 transaction.
- The system checks authorization objects when selecting certain functions in the transaction, nevertheless they are not reported correctly in the SU24 transaction, thus, they are not included in the corresponding role.

When the Authorization check fails because of access denial, we can use the following tools for determining the solution to this access:

- Using **Last Failed Authorization check** – transaction SU53
- Using Assignment of Authorization Objects to Transactions – transaction SU24
- **Tracing the Authorizations** for a function – transaction ST01

See more about the transactions SU53 and ST01 in the Appendix C**.**

6.5.3 User Access Management: ARM

Users need to verify that they have the right privileges to access the system. If users do not have access to transactions or operations they should, they will request it to the Security team involved in SoD & GRC.

These users' requests are usually handled through PaaS ticketing platforms specialized in IT Service Management, such as Service Now. These type of tools manage user requests and enable incidents reporting. These tools manage processes that are auditable and verifiable. In addition, they ensure a clear approval process, that checks for SoD violations, and if there is none, it provides and assign the appropriate role.

SAP offered under the GRC umbrella its own product, ARM (Access Request Management). ARM mainly consists in roles provisioning to users. Users need transactions that are not included in their existing roles or in roles that could lead to SoD conflicts.

ARM also has a workflow. Requests first need to be approved by the user line manager. Then, it is approved by the SAP Process Owner, who are in charge of assigning the user request to the Security team. The Security team is responsible for granting access to users. However, the role to assign will be first approved by the Process Owner and the Role Owner, as well as by Internal Control.

6.6 Maintenance

The maintenance phase starts when the SoD project has already been built in the Production environment. Real-time data is now being operated in the system. The testing phase has been approved, so there is no need to rollback.

However, over time, there will be changes in the system. Risks evolve and our company has to be able to adapt agilely in order to prevent any fraudulent activity in the system.

Risks are continuously being recognized and assessed through SAP GRC ARM. This tool will provide us remediation to SoD critical conflicts.

BRM will be also involved in the maintenance of roles, since there will be many changes in the system: new roles, transactions, mergers, and changes in job positions, inter alia.

User requests, tickets and incidences are tasks that require more time in the maintenance phase. ARM or a similar tool will help Security consultants to make this activity easier and faster to handle.

6.6.1 Privileged access for critical tasks: SAP EAM

The last SAP GRC Access Control functionality explained in this document is SAP EAM.

SAP EAM stands for Emergency Access Management, previously known as SPM Superuser Privilege Management or Firefighter (FF).

Users may require urgent access for exceptional circumstances. In these situations, the Firefighter user is a secure and auditable solution.

The Firefighter ID is a user ID that grants access in an exceptional basis. The FF ID is created by the Security team, and assigned to users or group of users (even departments) who require to carry out tasks in extraordinary occasions.

In these emergency situations, users log in to the FF ID and a prompt message will appear. Users are required to specify the reasons of use and the activities that are being performed from the FF that cannot be executed by their normal users because of lack of access, or access denial.

Once the information for the FF logon has been completed, users (logged in the system as FF) can execute these transactions. When users have finished these emergency tasks, they log off from FF ID and can continue with other activities from their normal users.

Additionally, every transaction executed by FF ID is reported to the FF Administrator, which will receive a complete report of the FF operations.

The Security team has to configure and create specific roles for the FF ID that will contain additional roles that are not authorized in a regular basis. However, there will not be authorized activities/functions which are not related to the position or department.

SAP EAM stands out for its versatility for users, besides being an easy and fast application to deploy in the system. The disadvantage of this tool is that users have to be trained on using the Firefighter only in emergency situations, and not as frequent use.

On the other hand, it is relevant that FF Administrators and FF Owners are formed to be capable to understand the transactions and operations which are reported by SAP GRC Access Control EAM.

7 PLANNING AND COSTS

In this section, it is presented a detailed vision of the project planning based on monitoring reports along the progress of the project. In addition, the total budget of the thesis is also broken down specifying each category of costs that apply.

7.1 Project Planning

The elaboration of this thesis extends from 1st January 2016 until 18th June 2016.

The following table shows the breakdown of planning followed for all the activities during the development of the thesis, indicating the time spent on each.

Task / Activity	Start Date	Duration	End Date
Study on the preliminary concepts	01/01/2016	13 weeks	31/03/2016
Analysis of Fraud and causes	01/04/2016	2 weeks	15/04/2016
Solutions: Regulation and Security Principles (SoD)	15/04/2016	1 week	22/04/2016
Design of a risk based-approach to SoD	22/04/2016	2 weeks	06/05/2016
Methodology of a project based on the design proposed	06/05/2016	3 weeks	27/05/2016
Documentation	01/04/2016	11 weeks	18/06/2016
Review and corrections	27/05/2016	2 weeks	10/06/2016

Table 18: *Project Planning. Source: Own elaboration.*

Following up the schedule planned on the table above, during the first three months, there was a previous analysis of the SAP security architecture and how SoD was structured and implemented, and a thorough research on GRC and SAP GRC tools. During this period, the emphasis was not dedicated on documentation, but in the previous research and analysis of these tools, so the average work for this period was around 2 hours per day.

The estimated hours in the first 3 months (90 days ~ 13 weeks) are calculated as:

$$13\ weeks \times 5\frac{days}{week} \times 2\frac{hours}{day} = 130\ hours$$

After this period, an average work of 6 hours per day have been dedicated to this project without taking into account holidays and occasional free days. The documentation was performed while detailed tasks were performed (analysis, solutions, design, methodology…)

The estimated hours in the last 3 months (77 days ~ 11 weeks) are calculated as:

$$77\ days \times 6 \frac{hours}{day} = 462\ hours$$

The project duration has an estimated amount of 592 hours (130 hours from the first phase and 462 hours from the second phase of the project).

7.1.1 Monitoring Reports

In order to evaluate the progress of the project, the development of the last 3 months have been measured along three different monitoring reports. The objective of these reports is to evaluate the progress of the thesis and focus on the tasks that were estimated to be completed in a certain date. In addition, it brings a complete vision of the project. It was a helpful tool for reviewing the thesis with its tutors along the project.

The result of all the monitoring reports is the burndown chart, which is a graph that compares that planned progress over the months with the actual progress of the project. This comparison is made in terms of percentage of the completed project, considering that each task has a specific weight based on the estimated days.

The blue bar (or line) shows the evolution planned early in the project based on the different tasks and estimated time it would take each.

The red bar (or line) shows the completed work until the day of the monitoring report.

These monitoring reports were distributed over time: on April 15th, on May 15th and on June 15th.

The first monitoring report was performed on April 15th, when the documentation had started, and the preliminary concepts had already been analyzed and documented.

In this first report, the project was under schedule, so tutors expected this work rhythm to continue along the project.

However, some tasks such as the analysis of fraud and its causes took a lot of time because of the thorough research on accounting cases and cybersecurity cases where fraud was involved.

Identifying the causes of fraud in each case and analyzing weaknesses of the firms affected and, then, finding solutions for preventing fraud took a long time, more than estimated firstly.

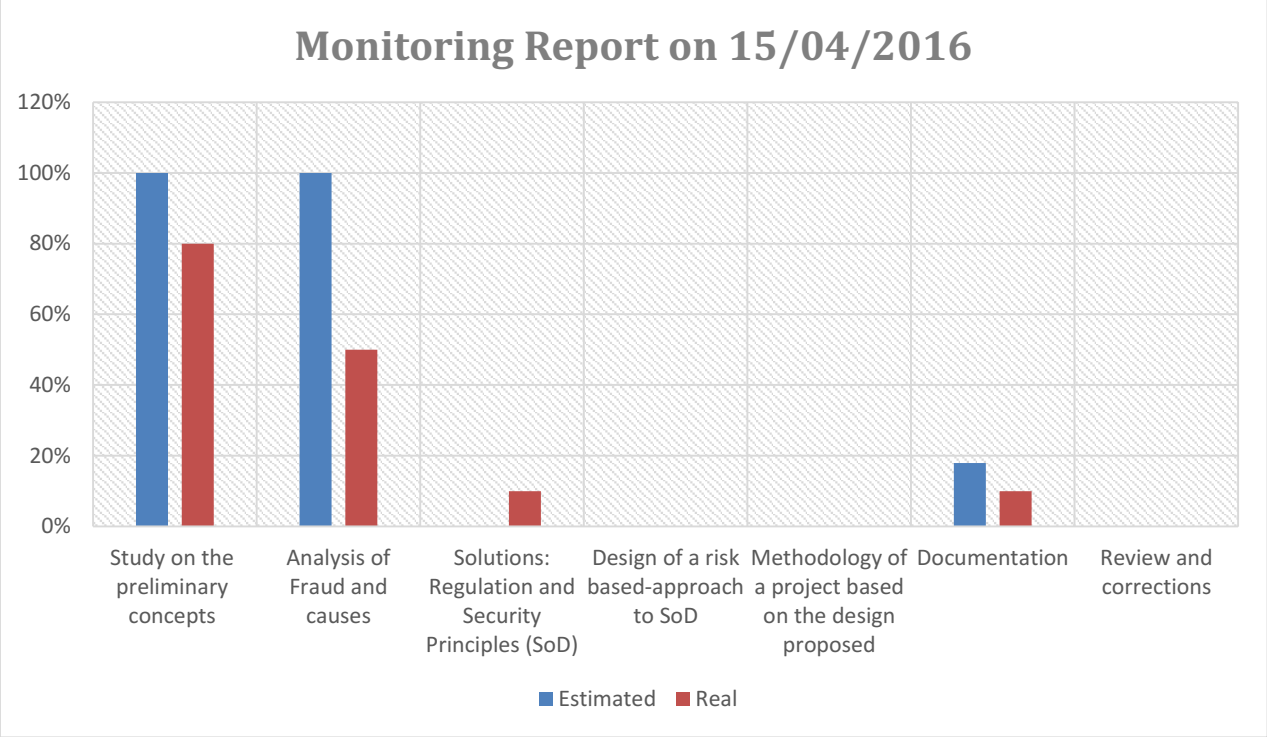


Figure 30: *Monitoring Report on 15/04/2016. Source: Own elaboration.*

The second monitoring report was performed on May 15th. The first tasks such as preliminary concepts, analysis and solutions were already carried out, however the design of the approach to SoD was about to be completed.

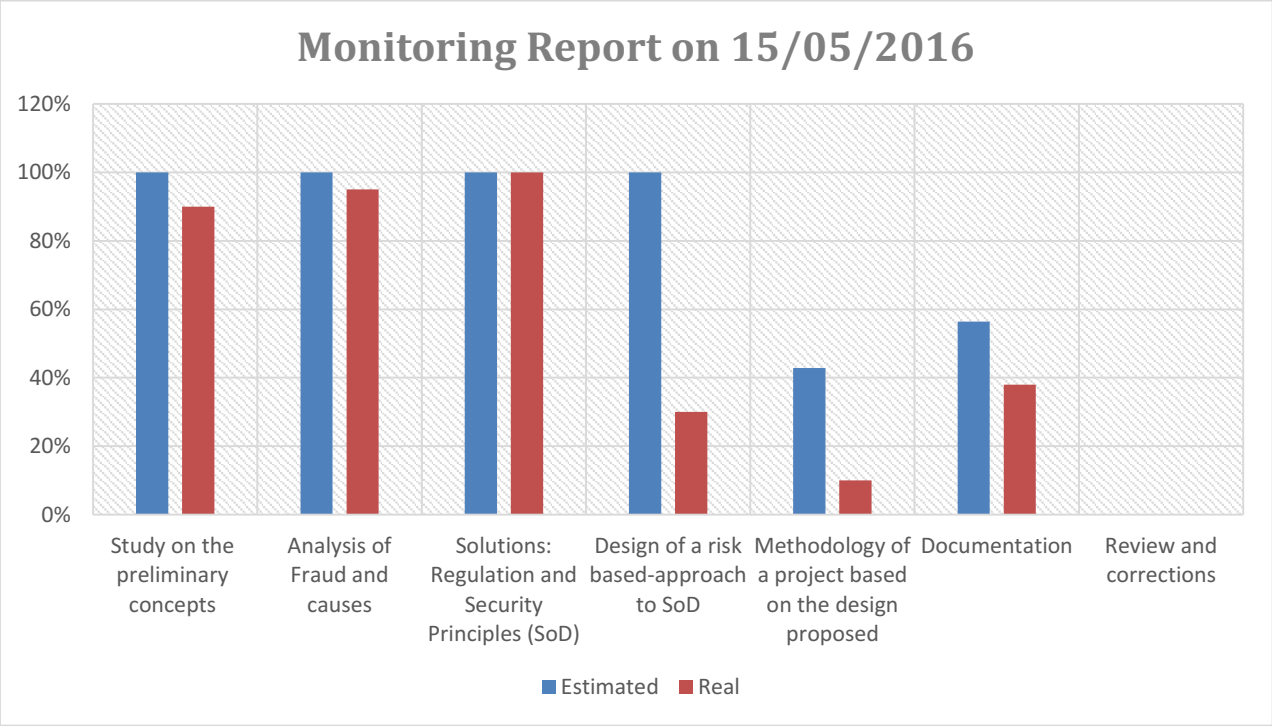


Figure 31: *Monitoring Report on 15/05/2016. Source: Own elaboration.*

However, the methodology was not advanced as it was estimated, since the design of the solution based on SoD from a risk-based approach required time and effort for streamlining tasks in relation to risk mitigation. In this phase, the project suffered high delays on the Design and the Methodology implemented. These tasks were completed at the end of May, contrasted and reviewed with tutors on several meetings.

The last monitoring report was carried out on June 15th. In this report, the project was almost completed. The thesis was adapted taking into consideration some tutors' recommendations.

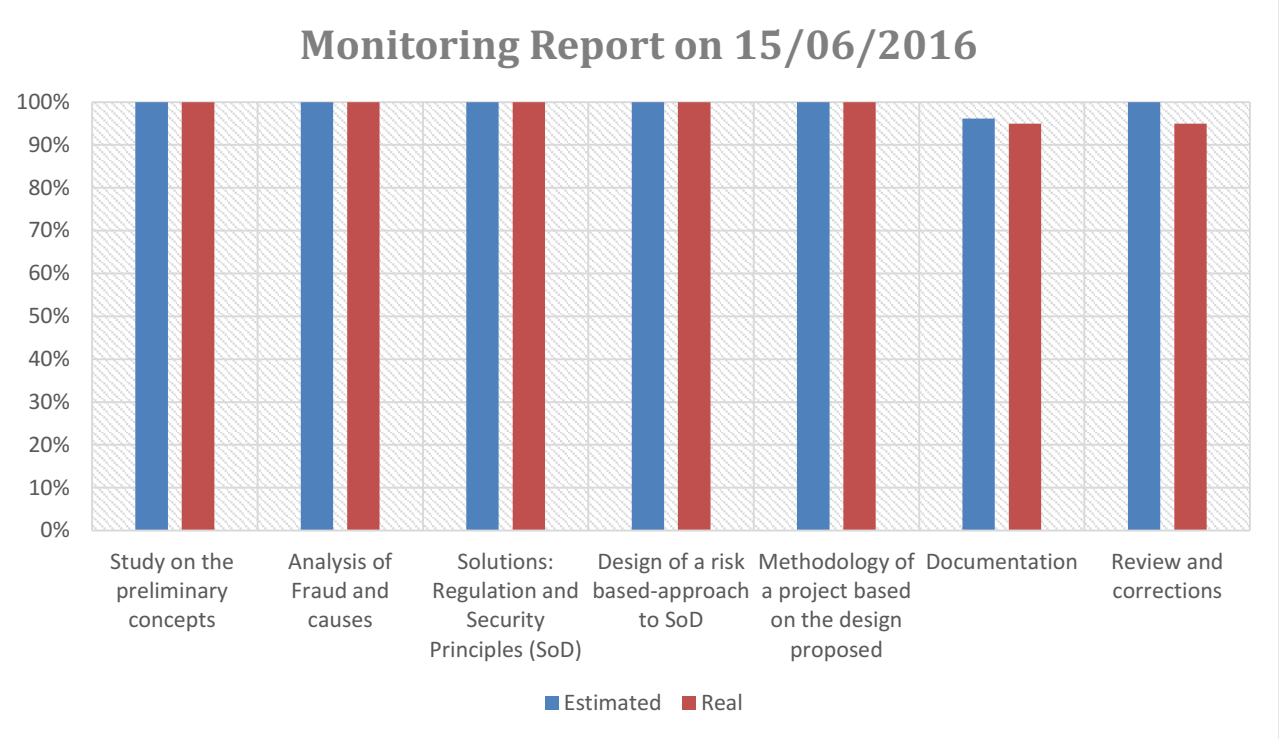


Figure 32: *Monitoring Report on 15/06/2016. Source: Own elaboration.*

Globally, most of the project progress was performed during April and May. Nevertheless, the analysis of the preliminary concepts of the thesis were documented in the first period of the thesis (Jan.-March). Last changes of structure, content and last sections such as conclusions and summary were documented on June.

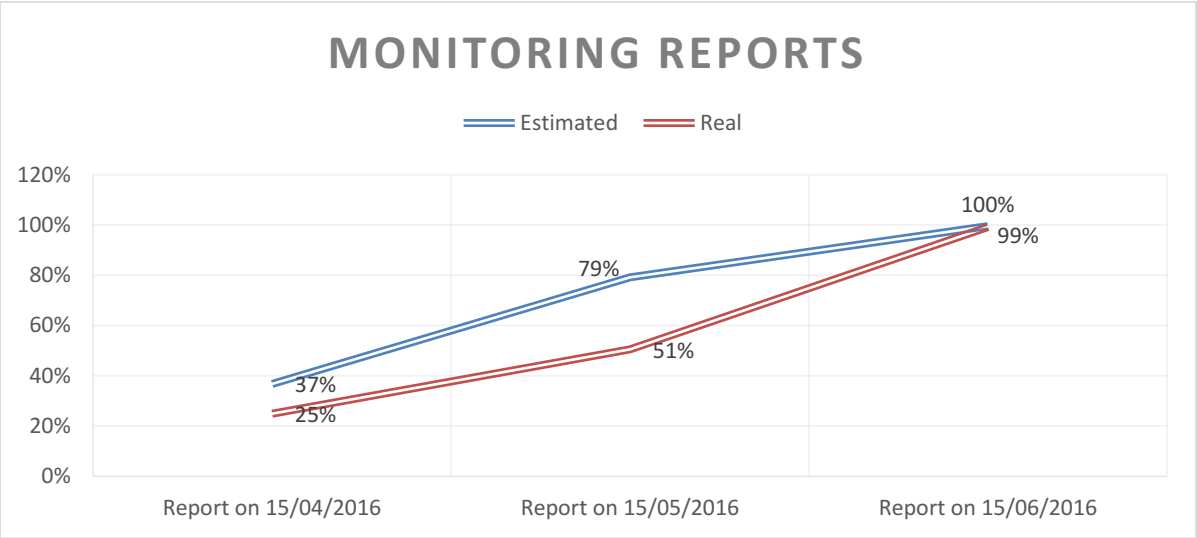


Figure 33: *Burndown chart: Progress on Monitoring Reports*

7.2 Project Costs

This section presents the estimated budget required for the development of the present project divided into categories.

7.2.1 Personnel cost

Taking into account average salaries of IT Security and Risk consultants in companies as PwC, EY or Deloitte with less than 3 years of experience, the average salary is around 22,000€/year. These salaries correspond to job positions in Madrid.

The duration of this thesis has been estimated in the project planning section to be approximately 500 hours. Based on a working day of 8 hours and 40 hours per week:

$$\frac{592hrs}{\frac{8hrs}{day}} = 74\ days;\ \frac{74\ days}{5\frac{days}{week}} = 14.8\ weeks$$

The duration of this project would be 62.5 days or 12.5 weeks working in a full time job.

Considering that the average number of weeks worked are 52 per year, the total personnel cost results in:

$$\frac{22{,}000\ €}{year} \times \frac{14.8\ weeks}{52\ weeks/year} = €\mathbf{6,261}$$

7.2.2 Hardware cost

The hardware devices used for this project consisted in two laptops: an enterprise laptop used to research on SAP security configuration and testing on SAP GRC Access Control,

and a personal computer to document the whole thesis and research on fraud and its analysis.

The enterprise laptop was a Dell Latitude E6230 Intel Core i5 2.60Ghz, 8GB of RAM and 120GB SSD, whereas the personal laptop used was a Sony VAIO Vpccb Intel Core i5 2.40Ghz, 6GB of RAM and 640GB SSD.

The cost computation for these elements has been calculated taking into account the depreciation period. The expected life of the enterprise laptop has been estimated to 3 years, while the expected life of the personal laptop has been estimated to 6 years.

The costs for these devices can be calculated by using the following formula:

$$Imputable\ cost = \frac{Cost\ without\ taxes}{Depreciation\ Period} \times utilization\ time$$

- Enterprise laptop:
  - Cost without taxes = €400
  - Depreciation period = 3 years ~ 156 weeks
  - Utilization time = 1st January 2016-31st March 2016 ~ 13 weeks (90 days)
  - $Imputable\ cost = \frac{€400}{156\ weeks} \times 13\ weeks = €\ 33.33$

- Personal laptop:
  - Cost without taxes = €700
  - Depreciation period = 6 years ~ 312 weeks
  - Utilization time = 1st April 2016-18th June 2016 ~ 11 weeks (78 days)
  - $Imputable\ cost = \frac{€700}{312\ weeks} \times 11\ weeks = €\ 24.68$

The total cost incurred in hardware devices are **€58.01.**

7.2.3 Software cost

The software used in the enterprise laptop for the thesis research were mainly the SAP GUI license and access to the enterprise SAP GRC Sandbox (which is a SAP testing environment separated from a real time production environment).

SAP GRC Sandbox and SAP GUI licenses are costs known by the enterprise IT team, but not public for the rest of the enterprise. The cost of a SAP license for an end user is around €990. Since SAP GRC Sandbox is not a productive environment and there is not real-time data connected, it has been estimated a 10% of its cost, €99 yearly. Bearing in mind that the firm software was used for 3 months, its cost has been approximated to **€25**.

In the personal laptop, the main tools used have been:

- Microsoft Office 365: Free of cost for UC3M students
- Gliffy (Online Diagram and Flowchart Software): Free of cost
- Windows 10 Professional License: Free of cost

7.2.4 Other costs

Indirect costs are included in this category, since they are costs not directly accountable to the cost object, such as electricity for the devices used and other office supplies. In order to provide electricity or fulfill other office supplies, there has been estimated a percentage of the direct cost budget for such costs.

It has been determined a 20% of the direct costs. In addition, there have been added two more cost elements in its calculation:

- Benefits, because of the advance and thorough research on SoD in SAP projects and its implementation. It has been considered a 15% over the costs.
- Risk Margin, 15% of direct costs has been assigned to risks that affected the project scope.

7.2.5 Total costs

The table below represents the costs involved in the thesis elaboration. In the bottom row, it has been estimated the total project cost. 21% of taxes have been added to the total cost.

Description	Cost
Direct Cost	**6,344.01**
Personnel cost	6,261
Hardware cost	58.01
Software cost	25
Indirect Cost	**634.401**
Electricity and office supplies	634.401
Total before Taxes and other Costs	**6,978.41**
Benefits	1,049.76
Risk Margin	951.60
Total before Taxes	**8976.77**
Taxes	1,885.12
TOTAL	**10,861.89**

Table 19: *Total Costs in Project Planning. Source: Own elaboration.*

As a result of the above calculations, the final cost of this thesis amounts to a total of **€10,861.89, taxes included.**

8 CONCLUSIONS

In the digital era, it is not surprising that risks arise from this technological world and fraud emerges when access control policies are trespassed. However, many companies are still unaware of the importance and the impact of these risks, and do not know the right measures to prevent them. The techniques to achieve an approximated assessment of risks is not so obvious for many companies and lies on a simple statement: Segregation of Duties.

Segregation of Duties (SoD) offers a solution to fraud by separating tasks that when combined together come into conflict. This methodology provides job positions categorized as roles with minimum privileges throughout the entire business concept. Business processes are the core of this methodology. That's why companies which do not pay attention to how their business processes are integrated and how its departments communicate with each other will not be able to create a consistent work environment for tasks, applications, and most importantly, people.

Access control policies play an important role while building a SoD model. The SoD process proposed follows a Roles Based Access Control architecture. This security approach consists of two main principles: minimum least privilege and prevention of SoD conflicts.

This thesis started with the focus point on ERPs, such as SAP. ERP systems offer an integrated vision of all the business processes across the organization. They allow to identify and manage the main tasks of the company. Business processes have to be streamlined and coordinated to provide consistent and automatic workflows. Such workflows are the most important tool to enable a correct segregation of duties.

ERP avoids different business applications and gathers all the information in a single software where information is real-time, accurate and integrated. This results in a higher employee efficiency and better quality in our results. One of the ERP advantages is being able to easily trace and report information. In this way, these systems can trace and monitor critical tasks favoring fraud detecting.

In addition, ERP solutions provide a complete security configuration based on different levels of access. SAP, as one of the most popular ERP examples, has been an adequate example thanks to the authorizations structure that offers.

Our research question has been to analyze fraud in real cases where enterprises have faced financial and fraud crimes, as well as cybersecurity attacks. Fraud has been studied from its origin to identify conditions that cause the occurrence of fraud.

The result was a combination of the Fraud Triangle by Wells, J.T. 2005, and the Fraud Diamond, by Lormel, D. 2012. These philosophies of fraud present different causes of fraud that together structure all its components: motivation, opportunity, capabilities and personal integrity.

From these fraudsters' reasons to commit fraud, this study extended that this causes must be analyzed from an individual and enterprise structure. There are many pressures and motivational causes that can lead employees to commit fraud, as well as its capabilities in the company or its rationalization. However, there is another element that depends to a large degree on companies, that is opportunity. Opportunity relies heavily on the enterprise opposition to fraud and the security measures it provides to prevent it. Companies should not leave the door open to opportunity, because that is what will make fraudsters to endanger your business. At the end of the document, there have been listed some recommendations for enterprises to prevent fraud based on the 4 dimensions that fraud can arise from.

Through a review of different notable cases where accounting fraud was involved, there have been analyzed for each particular case its causes for committing fraud, the fraud strategies carried out and some weaknesses that companies had. The results evidenced the main failures of companies. Firstly, weak supervision and control over capable positions such as top management and the accounting department. Secondly, lack of internal control procedures. Thirdly, it was identified an unhealthy corporate culture that incentivized bonuses unrelated with employees' performance, besides an unclear definition of goals and no established thresholds for compensation. In addition, there was not defined any code of ethics and conduct in the company. This denoted an individualist environment that did not encourage cooperation and teamwork. Last but not least, lack of access control was a common factor in all companies examined.

The latter point was the common factor in the companies analyzed that were heavily damaged by computer cyberattacks. Hackers and fraudulent employees took advantage of lack of access control tools that companies had. The most popular strategies were to access to critical data using some employees' credentials and then installing sniffer malware on the network of the application. Employees' unconsciousness of the risk that ID credentials pose is a key factor that companies need to prevent. Many fraudster and hackers sold then the data stolen to ID thieves. Internal security measures were insufficient in all the cases in order to protecting critical users' data.

As hackers access with users' credentials, it is crucial that from these user accounts, hackers are not capable of performing any critical task in the system, and even less to manage all phases in a transaction such as recording, authorize and settle a transaction.

Due to the large amount of cases regarding financial fraud through cyberattacks and malware, the value that this research brings to companies is remarkably high. Moreover, the economic figures of these attacks have been taken in consideration since the losses assumed by the companies concerned exceeded billion dollars.

As a consequence of these cases, numerous regulations have emerged to prevent fraud. The regulations that deal with internal control and corporate governance as well as the security policies related have been included in this document. Regulations such as COSO and SoX strengthen internal control rules and implement higher control over CEOs and CFOs operations.

SoD from a risk based approach

The solution for companies to prevent fraud is implementing a model based on Segregation of Duties from a risk approach. Through this study, it has been analyzed the SoD process in accordance to the risk lifecycle, due to the fact that SoD is built from conflicts between tasks, which pose a risk to enterprises. These conflicting tasks are separated into different roles to ensure separate responsibilities and privileges.

The SoD process embodied in this research starts with the risks identification, then an analysis of risks and its prioritization, which will lead to assess and evaluate the impact of the risks that affect our firm. Defining functional and technical matrixes will help us to identify SoD conflicts in the system. The next step is to create some rules that mitigate such risks. Fraud risks will be controlled and automatized in the rules defined, that will be collected and processed in tools such as SAP GRC Access Control. Then, these risks will be continuously monitored to prevent future fraudulent operations and create alerts when attempted.

GRC: Collaborative workplace

Another concept that enhances SoD from a risk perspective is the GRC term: Governance, Risk Management and Compliance. The lesson learned from its benefits is the importance of a collaborative work environment where different departments have to cooperate together to ensure a correct SoD. Security analysts do not know what business processes are relevant in the business or where there can be SoD conflicts and possibilities of fraud, but Internal Control do. Risks can only be assessed and identified by a Risk Management team, as well as the Security department will be involved in the configuration of the SoD process attending to the security implemented in the organization. All these tasks have to be audited simultaneously by Audit Management that will ensure that these activities have been correctly reported attending to accounting standards and application controls over IT security.

SAP GRC Access Control as a powerful tool to control risks and enhance SoD

SAP GRC Access Control has been the tool used to design an architecture project based on the key concepts mentioned: SoD, risks and GRC. In this research, it has been reflected how a project implementing SoD would evolve by using SAP GRC AC. An analysis of the tasks executed allows to define different roles: functional roles, organizational scoped roles and business roles. The described project is implemented through the following phases: a previous analysis of SoD, design of roles with the corresponding authorizations, implementation of these roles and rules of control, testing and a continuous monitoring. For each of these stages, there is a tool that can be used in SAP GRC Access Control, such as ARM for risk identification, BRM for business role management, EAM for critical tasks auditing and monitoring, and ARM for user requests of access incidences in the system.

To sum up, fraud and cybersecurity attacks have been assessed by developing a role based access control architecture that develops as a security control segregation of duties in the business processes. In order to achieve this model, there has been proposed a SAP project which employs the module GRC Access Control to build security privileges from a risk-based approach.

8.1 Recommendations and future development

Lastly, there have been developed different measures to help enterprises to prevent fraud. These recommendations are based on each area of the **New Fraud Triangle Model** (Kassem & Highson, 2012) described in Section 3.1, which are: motivation, opportunity, integrity and fraudster's capabilities.

Capability*:* People with top positions in organizations or authoritative functions can be influenced to commit fraud because they are more capable to do it. These positions should be more controlled than others in terms of their security access. These highest levels of the organization should lead by example and respect the ethical standards of the company.

Motivation: The company should push for employees to not commit fraud through measures such as the following:

- ✓ Compensation structure based on objectives and milestones
- ✓ Non-financial incentive plans such as additional paid vacations or increased professional development
- ✓ Establishment of sales incentives based on profits, not revenues

- ✓ Salary commensurate to the market and to the job position played
- ✓ Managing work place frustration by analyzing and treating these cases

Due to the fact that nowadays firms must be profitable, there is no room for failure and if managers or some employees do not meet their objectives, they will be dismissed from office. To prevent unfaithful employees and high staff turnover, it is very valuable to invest time and resources on increasing the sense of belonging to the company.

Integrity: In order to provide a positive and respectful work environment, where fraud is prevented, these could be some solutions:

- ✓ Staff training and continuous assessment on fraud issues
- ✓ Establishment of anti-fraud programs: code of ethics, policies, procedures…
- ✓ Determination of lines of complaints

Opportunity: Business processes must be diagnosed, analyzed and evaluated for the purpose of covering any possible security breaches for fraud. These evaluations could be the following:

- ✓ Specialized audits that meet the current regulations
- ✓ Third parties continuous monitoring and management of payments
- ✓ Evaluation and constant updating of risks and controls

The formula to protect businesses from fraud is not unique, it depends on many critical factors, as we have listed. However, there is a key point for both small and large companies: identify and assess each of the risks and mitigate them. Combating fraud is how we help building a better business workplace for all.

9 Executive Summary

Large scandals where fraud is involved has become the main reason for enterprises to get protected from risks within the enterprise. Internal risk controlling is an area that is being exploded over the last years due to its importance for analyzing risks and mitigating them through security controls.

On one hand, governments are forcing enterprises to comply with certain regulations for internal control and a responsible corporate governance. On the other hand, fraud must not only be understood as compliance with applicable regulations, but as a whole process to identify risks affecting our company and design and develop an action plan to control these risks and mitigate them. It is important that enterprises focus on this challenge as an **evolutionary and adaptive process** over time but not as a straight temporary project. Firms have to be totally aware of the importance of preventing risks, so they can invest a significant amount of their budget in control and protection.

Fraud has to be studied from its origin, so it can be explained why fraudsters commit it. In this way, enterprises can determine which areas to be reinforced due to security holes or weak motivation measures.

In search of the **causes of fraud**, there have been analyzed different theories. Firstly, a theory that describes three sides of a fraud triangle, which are opportunity, rationalization and pressure. Then, this philosophy was studied and reviewed by researchers as Wolfe and Hermanson who added up another factor in this study: Capability. Fraudster's capabilities can be encouraged based on motivators such as Money, Ideology, Coercion and Ego (MICE theory). From all these perspectives, it was concluded that fraud can be occasioned from the combination of these 4 variables: **motivation, opportunity, fraudster's capabilities and personal integrity** (rationalization).

Taking into consideration all these factors, there is one side of the triangle that is highly relevant for companies, which is opportunity. Compared to the other factors, this variable is highly dependent on the fraud occurrence, since it relies heavily on the enterprise opposition to fraud and the security measures it provides to prevent it.

Through a thorough research on accounting scandals and data breaches were fraud is involved, there were some main reasons of fraudsters to commit fraud: the lack of **internal control policies and the capability of fraudsters** (hackers or employees) to commit fraud. These capabilities increased due to a weak and fast access to critical data using other employee credentials.

Once fraud is recognized, enterprises will need to analyze their weaknesses when protecting themselves from fraud. In addition, companies must bear in mind the applicable regulations regarding to internal control and corporate governance. Such regulations have arisen to prevent fraud and strengthen internal control policies in companies.

The solution to enterprises in the pursuit to prevent fraud is described in this thesis. This proposal is based **on a security architecture solution that is focused in Access Control**. It has been followed a Role Based Access Control model, which is focused on a security principle: **Segregation of Duties (SoD)**. Such user roles are formed with the necessary privileges for its job position tasks, so a user cannot have access to the whole process.

Segregation of Duties has been directed in this thesis as a process. This security principle consists on separating those tasks that may lead to a conflict, thus, to fraud. Such risks can be mitigated, however the business processes and their tasks evolve continuously and the firm has to be adaptive and monitor constantly risks. In order to understand this risk process, it has been analyzed SoD from the **risk management lifecycle**. All tasks involved in the SoD processes have been adapted to the different phases of risk management cycle: identification, analysis, assessment, action plan, implementation and monitoring.

As a result of the risk analysis over SoD performed, this process has been applied to the **methodology of a whole project.** Enterprises which are interested in implementing a SoD solution in their business core should follow this methodology for a correct segregation of duties evaluation and implementation. It is relevant that companies provide a streamlined set of business processes throughout the entire company. Companies using ERPs will be more ready for starting building SoD than unorganized enterprises that control many applications for different purposes.

From this point, the definition of **functional and technical matrixes** will provide information about the conflicts to evaluate and assess. Those SoD conflicts that pose higher risks for the company will be mitigated through **mitigation controls**. These can be automatically set up for building risks rule sets and alerts when the detection of any fraud risks.

The methodology of SoD has been conducted using the tools offered by **SAP GRC Access Control.** This software application is an integrated set of tools that helps enterprises to implement SoD through risk monitoring, auditing reports on critical tasks in the system, a role based access control model deployed and managed with business roles, and so on. It is relevant to note that this tool is structured from a GRC framework.

GRC (Governance, Risk Management and Compliance) can be described as a collaborative work approach that looks at the enterprise as a whole, integrating tasks from different departments and streamlining them in a unique solid system. GRC changes the work paradigm in the departments involved in Internal Audit, Risk Management, Compliance and IT security. All these areas work together from different perspectives but within the same integrated SoD process.

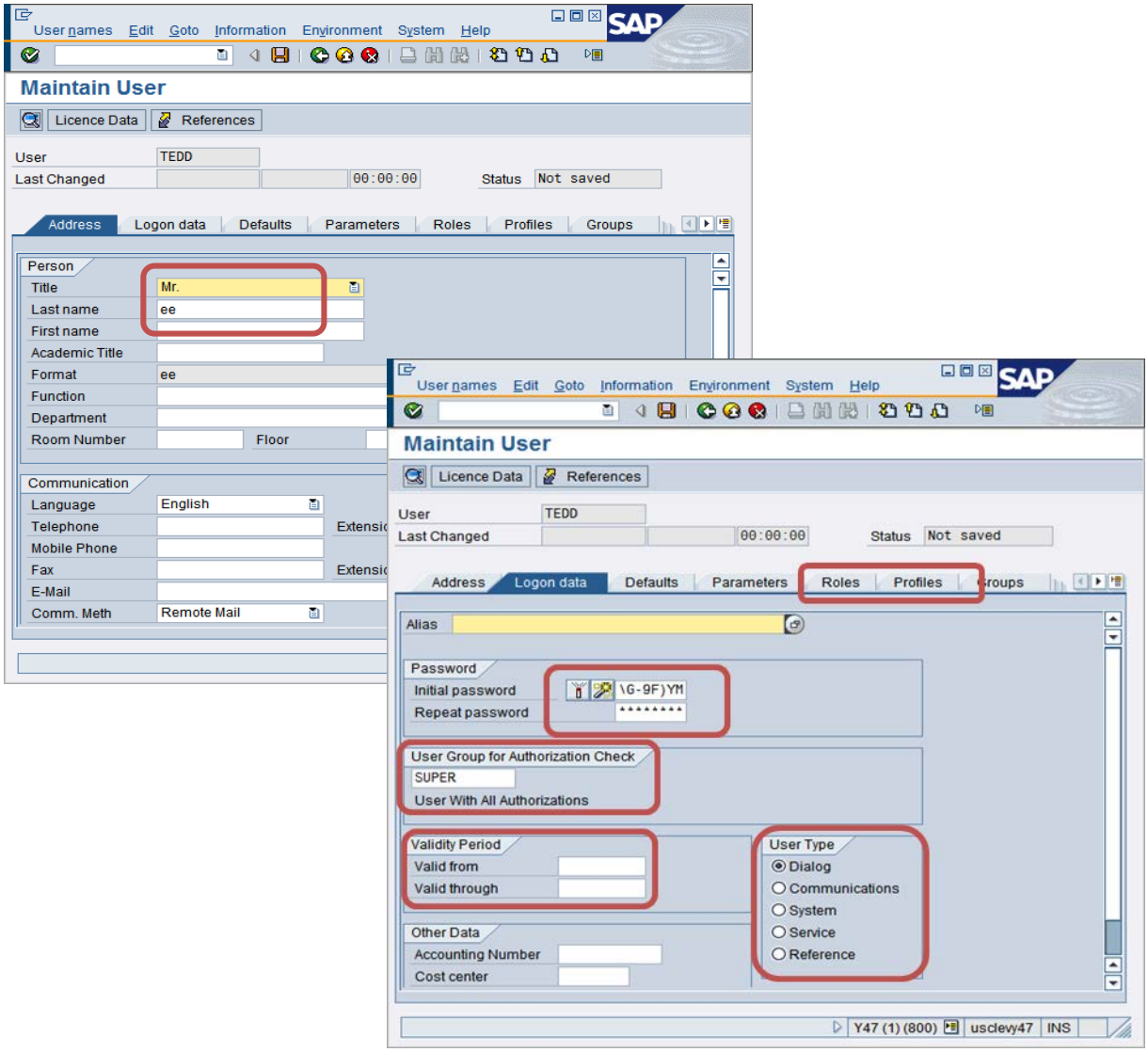
Compliance with internal control policies and applicable regulations is also crucial and these verifications are included in tools such as SAP GRC Access Control. Enterprises that install and maintain correctly a SoD methodology will be able to successfully comply with regulations regarding to corporate governance and internal control.

All the **measures proposed do not imply a large investment for companies**. As been analyzed in this thesis, all these regulations, security software and the personnel involved in a complete Segregation of Duties project represent only a 0.7% of the total losses resulted from a data breach. (Percentage shown in the worst case scenario presented: T.J.Maxx).

Companies should stablish a well-defined strategy to **build security measures** as proposed. In addition, it is recommendable to build a healthy corporate culture, a compensation structure based on objectives and milestones, control thoroughly the highest levels of the organization and perform staff training on fraud issues and security awareness, among others.

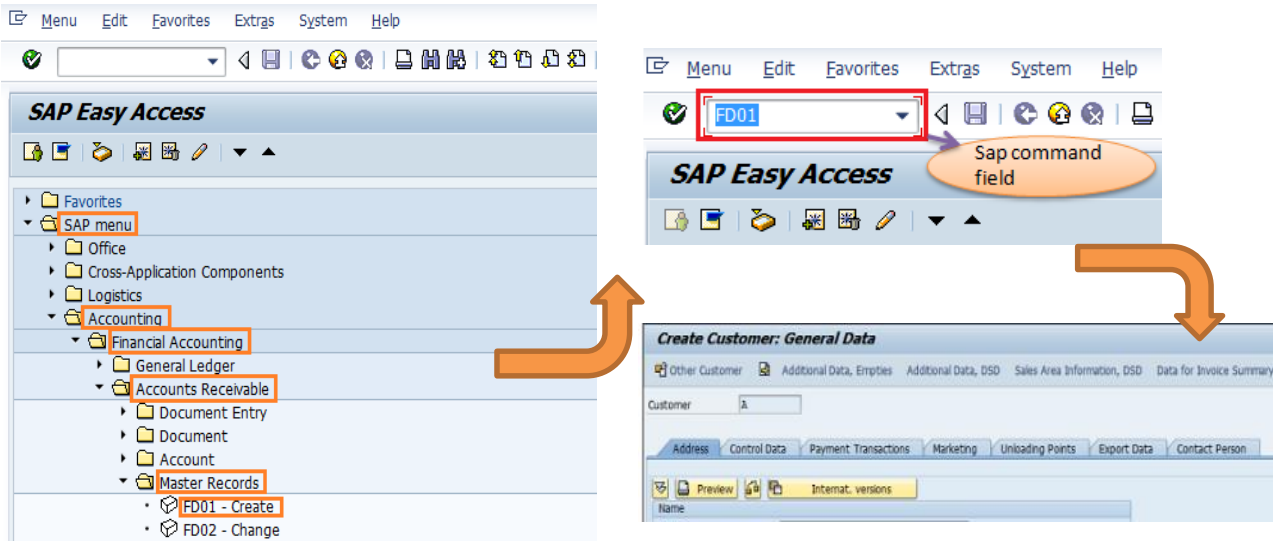
10 Appendix A: Additional SAP Security Configuration

1. Master Users' Records configuration from transaction SU01



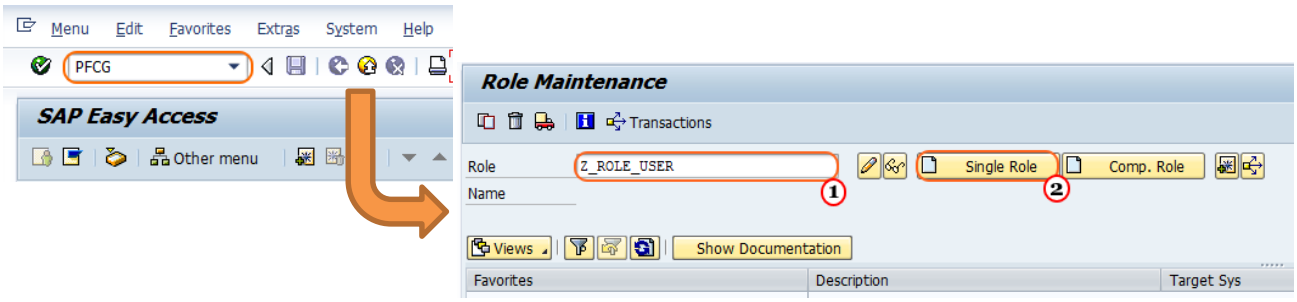
2. Example of access to a transaction by using its T-code

For example, the transaction FD01, which allows us to create customer master records, can be accessed through the SAP Path: SAP Menu > Accounting > Financial Accounting > Accounts Receivable > Master Records > FD01 – Create (See image at the left below). However, the fastest way to access is by entering the T Code in SAP. (See image at the right below).

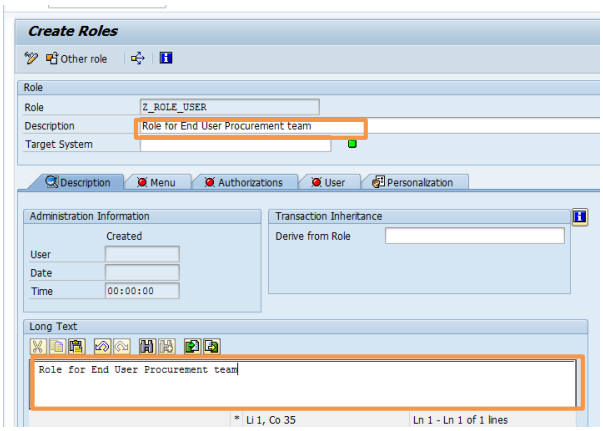


3. <u>Configuration procedure of a single role with transactions associated and its assignation to a user.</u>

In the image below, we show how to create a single role, which name is Z_ROLE_USER, from the transaction code PFCG.



Then, the role created is completed with a description about the role and a long text of the role.

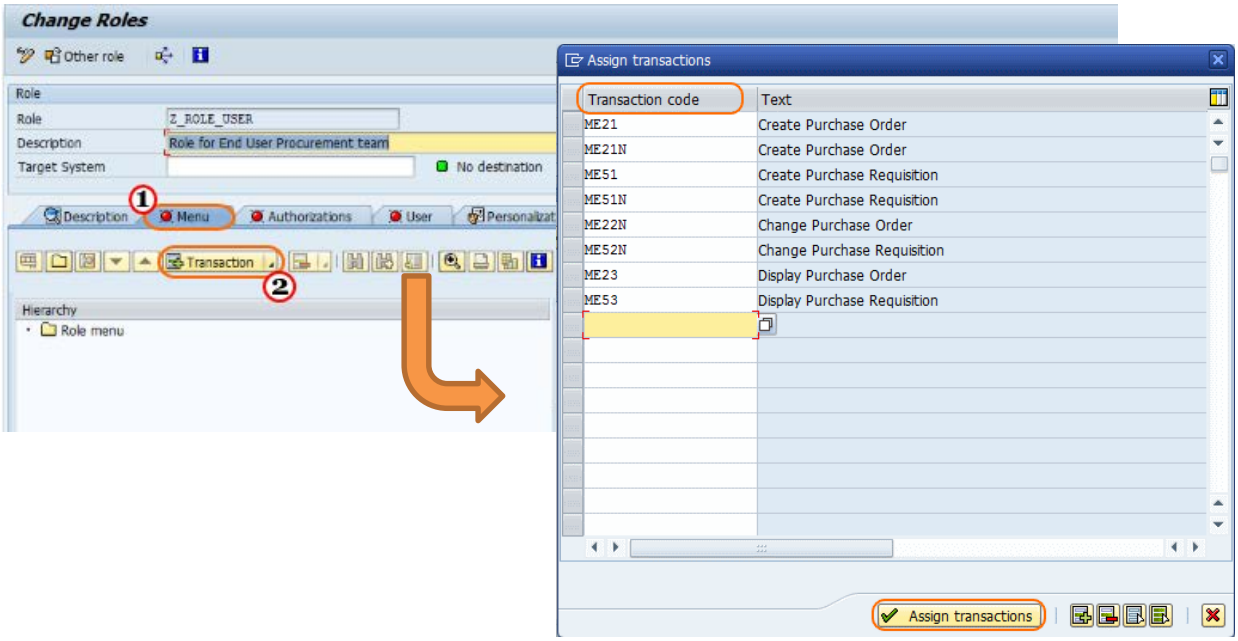


After these changes we save these details clicking on the save button.

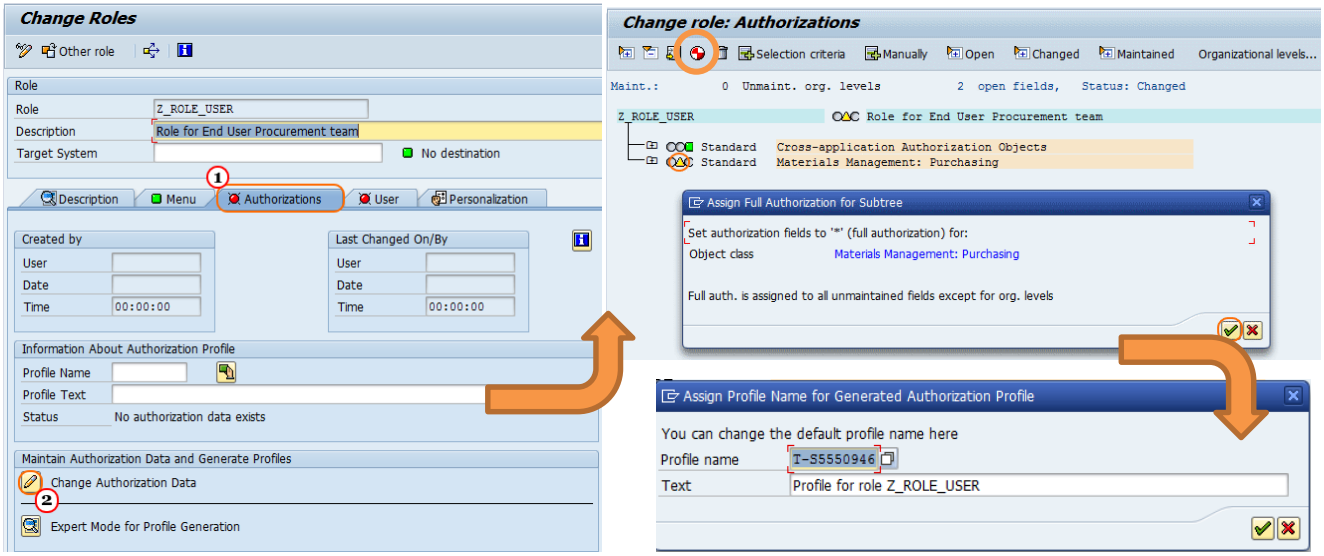
The next step is to assign transaction codes to the role. In this way, users who are assigned this role can have access only to the specified transactions on the role menu.

Selecting the Menu Tab (1), we can create folders and insert transactions (2).

In these folders, we can assign the transaction codes that are related to the role functionality. In the image at the right, there are transactions associated to a Buyer Position Role.

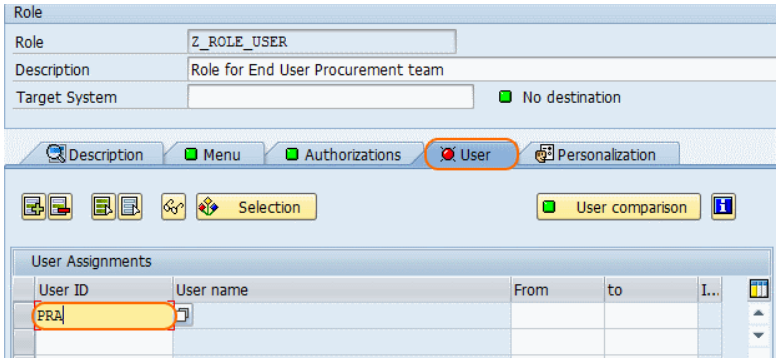


Then, in the Authorizations Tab, we click on Change Authorization Data in order to check authorizations contained in the profile of this role.



When selecting the round red cycle button on the settings, we will generate **automatically the profile** of the role.

The last step is to select the User tab, that allows us to assign this role to user IDs with a specified validity.

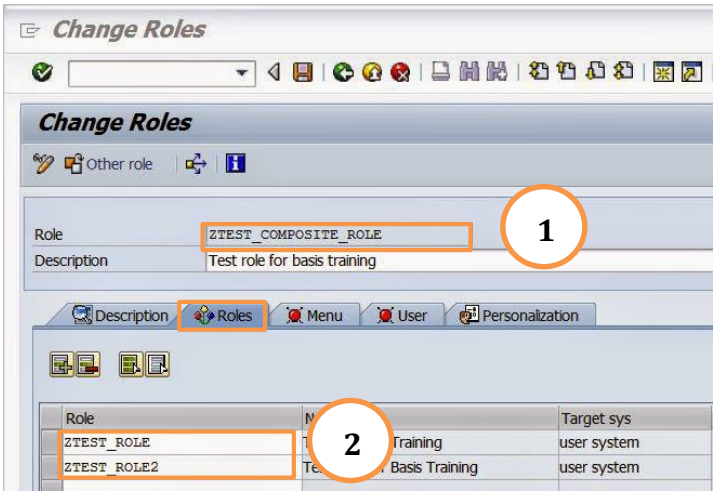


4. Configuration procedure of a composite role

In order to create a composite role, first we need to create single roles so we can add them in the composite role in the Roles tab (transaction PFCG in SAP).

Composite roles as well as single roles have to be define with a unique name. Role names, either single or composite, cannot be changed since its creation.

The composite role (1) will contain those roles (2) that are related and that can be associated forming a unique role.



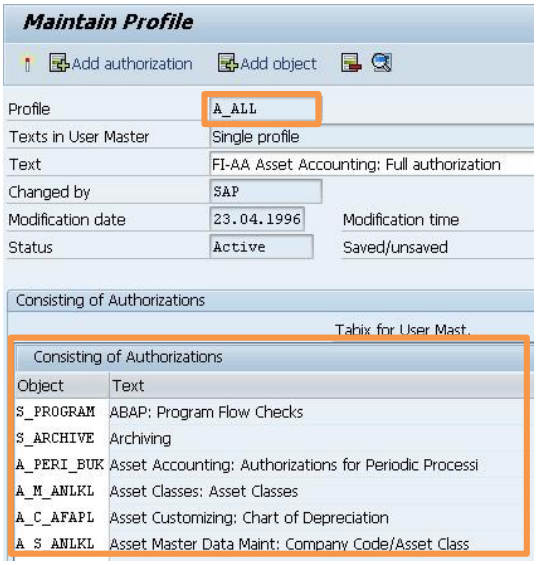
5. Manual profile generation

In the example used previously in the single role creation with the example role Z_ROLE_USER, we created its profile automatically using transaction PFCG.

By using **transaction SU03**, profiles can be created through a manual process. This process is time-consuming and requires expertise on the authorization concepts.

As we see in the image at the right, a profile consists of authorizations: authorization objects that include determined authorizations defined in the system.

The profile A_ALL consists of authorizations: authorization objects such as S_PROGRAM, S_ARCHIVE, A_PERI_BUK…



11 Appendix B: Analysis of authorization objects for SAP CO module

11.1 SAP Controlling (CO)

Controlling (CO) is the term used by SAP referred to **'Managerial Accounting'.** This is concerned with the provisions and use of accounting information to managers within organizations. This module provides managers the basis needed to make informed business decisions in order to achieve a better controlling management.

Managerial accounting, in contrast with financial accounting (FI), provides data for internal use of the enterprise. It emphasizes relevance and flexibility of data, and it has a long-term emphasis, easing managers to take well-versed decisions for the future. It is a means to an end.

Managerial accounting looks at the business as a whole, but it also focuses on different parts of it. This type of accounting draws significantly from other disciplines such as finance, economics, and operations research, that's why it is highly recommended to use the CO module in conjunction with other modules, such as FI, MM, SD, PP or HR.

Actually, the whole Accounting Module (FI-CO) plays the role of a 'Feeder System' since they are the core modules of SAP. Even if an enterprise is interested in implementing only the SD module and the CRM product, the FICO module will be basic since it is highly correlated to others, therefore, the complete FICO module should be the first module to deploy.

SAP recommends Controlling implementation to be carried out in three different phases: Foundation, Stabilization and then Enhancement and Optimization.

Controlling is divided into the following areas:

1. Cost Element Accounting (CO-OM-CEL): Component that controls in real time all financial transactions relevant to profit and loss accounts.
2. Cost Center Accounting (CO-OM-CCA): Sub module used for internal control of each cost center in the organization. The standard hierarchy of cost centers enables to visualize and control organization performance, based on the comparison of planned and actual costs for each of them. The client can set up a monthly budget for every cost center.
3. Internal Order Accounting (CO-OM-OPA). Internal Orders are normally used for managing small projects (internal jobs and tasks) that need to be budgeted and managed independently. They enable the client to plan, collect and settle costs of the project. It is helpful for top management on the decision-making process.

4. Activity-Based Costing (CO-ABC). This sub module allows to define more precisely of the origin of the costs associated with a particular process.
5. Profit Center Accounting (EC-PCA): Sub module used for management-related internal reporting. A profit center is a unit managed independently by a person who is responsible for the profit.
6. Product Costing (CO-PC): This sub module measures the material cost of a product, that is the value added by each process and organizational unit. It determines inventories and helps to take make or buy decisions.
7. Profitability Analysis (CO-PA): This tool allows the client to review information related to the benefit of the company, as well as the added value that provides a specific business segment.

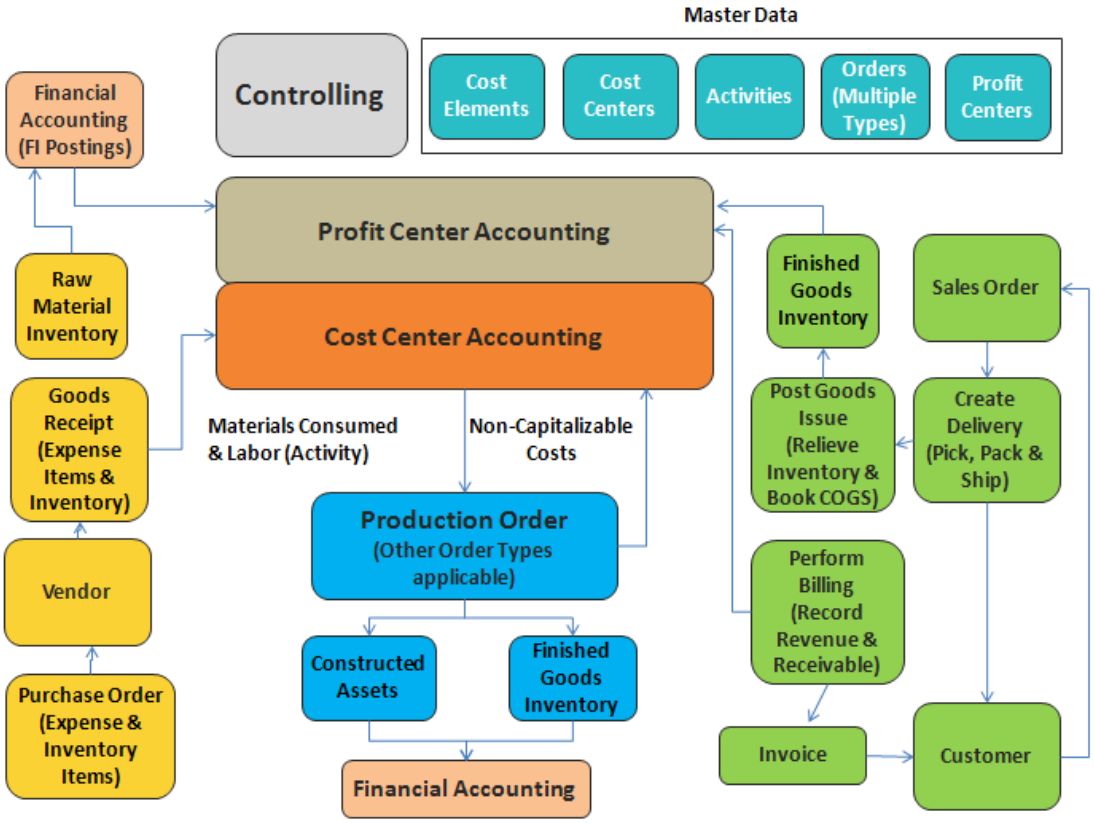


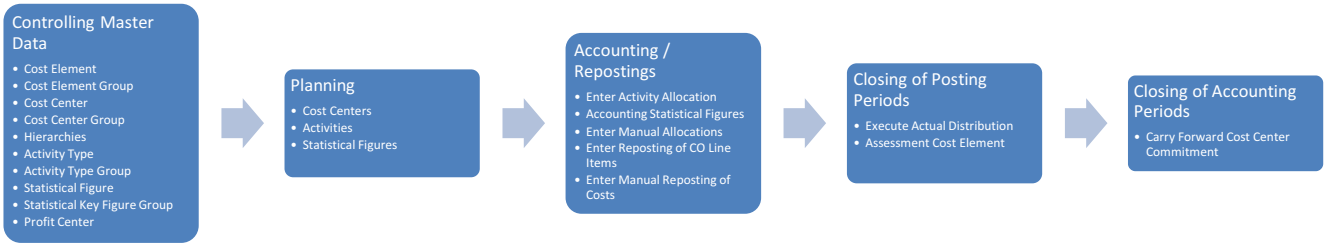
Figure 34: Controlling Structure (Garmendia, 2012)

11.1.1 Standard flow of the Controlling Business Processes

The main controlling activities that are being represented in the following flows are related to the **Cost Center Accounting** (CO-OM-CCA) and **Internal Orders** (CO-OM-OPA).

SAP Menu > Accounting -> Controlling -> Cost Element Accounting -> Master Data

- Cost Center Accounting flow



- Internal Orders Accounting flow

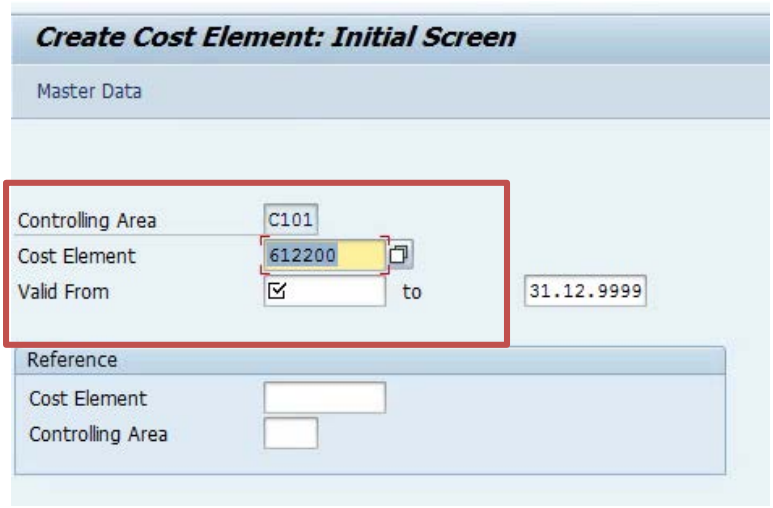
11.1.2 Authorization Objects Required

In this section, there are being listed the authorization objects required to have the proper access to the main transactions for the Controlling Module. The authorization objects needed have been detected after a previous analysis of the main transactions for the CO Module, that are the following:

SAP Transaction Code	Transaction Description
KA01/KA06	Create primary/secondary cost element
KAH1	Create cost element group
KAH2	Change cost element group
KS01	Create cost center
KS02	Change cost center
KS03	Display cost center
KSH1	Create cost center group
KO01	Create internal order
KOH1	Create internal order group
KP26	Change activity type/price planning on cost center
KK01	Create statistical figure
KBH1	Create statistical key figure group
KSCF	Carry forward cost center commitment
KL01	Create activity type
KLH1	Create activity type group
KB11N	Enter manual reposting of costs
KO88	Actual settlement: Order
S_ALR_87005757	Create distribution assessment cycle
KSU1	Create actual assessment

1. KA01/KA06 - Create primary/secondary cost element

   The authorization object for primary or secondary cost elements is **K_CSKB**. This authorization object protects the cost elements in master data maintenance.

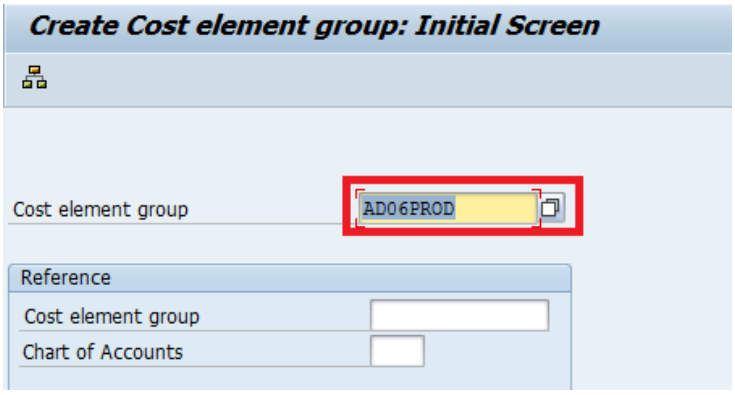


Authorization Object	Description	Fields	Values	Table	Role Type
K_CSKB	CO-CCA: Cost Element Master	ACTVT: Activity	01 – Role for creating the cost element	N/A	Organizational Role
		CO_KAINT: Cost Element Classification (Primary/Secondary)	1 – Primary Cost 2 – Secondary Cost	CSKS	
		KOKRS: Controlling Area (that belongs to a cost center)	Depends on the enterprise		

   Other activity values are 02 - Change; 03 - Display; 06 - Delete; and 08 – Display change documents.

2. KAH1 - Create cost element group

   The authorization object for creating cost element groups is **K_CSKA_SET**. This authorization object protects maintenance of cost element groups.

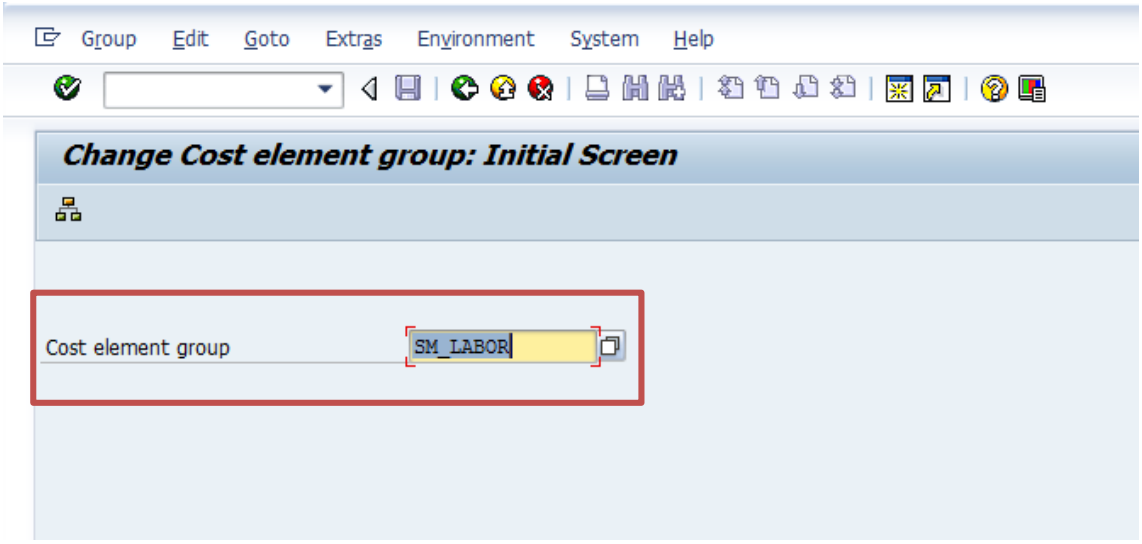


Authorization Object	Description	Fields	Values	Table	Role Type
K_CSKA_SET	CO-CCA: Cost Element Groups	ACTVT: Activity	Depends on the enterprise	N/A	Organizational Role
		KTOPL: Chart of Accounts	01 – Role for creating cost element groups	CSKA	

Other activity values are 02 – Change and 03 – Display.

3. KAH2 - Change cost element group

The authorization object for changing cost element groups is **K_CSKA_SET**. This authorization object protects maintenance of cost element groups.

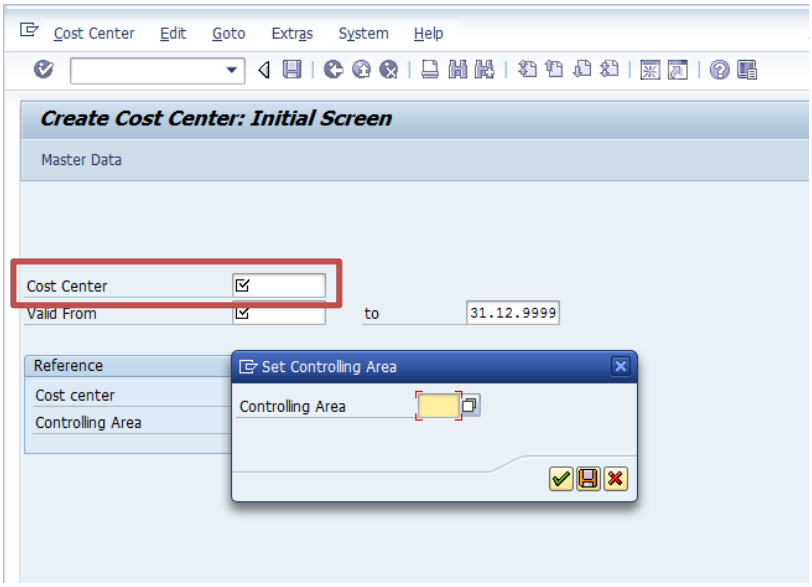


Authorization Object	Description	Fields	Values	Table	Role Type
K_CSKA_SET	CO-CCA: Cost	ACTVT: Activity	Depends on the enterprise	N/A	Organizational Role

	Element Groups	KTOPL: Chart of Accounts	02 – Role for changing cost element groups	CSKA	

4. KS01 - Create cost center

The authorization object for creating cost centers is **K_CSKS**. This authorization object protects the cost centers in master data maintenance for Cost Center Accounting.



Authorization Object	Description	Fields	Values	Table	Role Type
K_CSKS	CO-CCA: Cost Center Master	ACTVT: Activity	01 – Role for creating the cost center	N/A	Organizational Role
		KOSTL: Cost Center	Depends on the enterprise	CSKS	
		KOKRS: Controlling Area (that belongs to the Cost Center)	Depends on the enterprise		

Other activity values are 02 – Change; 03 – Display; 06 – Delete; 08 – Display; 63 – Activate inactive cost centers.

5. KS02 - Change cost center

The authorization object for creating cost centers is **K_CSKS**. This authorization object protects the cost centers in master data maintenance for Cost Center Accounting.

Authorization Object	Description	Fields	Values	Table	Role Type
K_CSKS	CO-CCA: Cost Center Master	ACTVT: Activity	02 – Role for changing the cost center	N/A	Organizational Role
		KOSTL: Cost Center	Depends on the enterprise	CSKS	
		KOKRS: Controlling Area (that belongs to the Cost Center)	Depends on the enterprise		

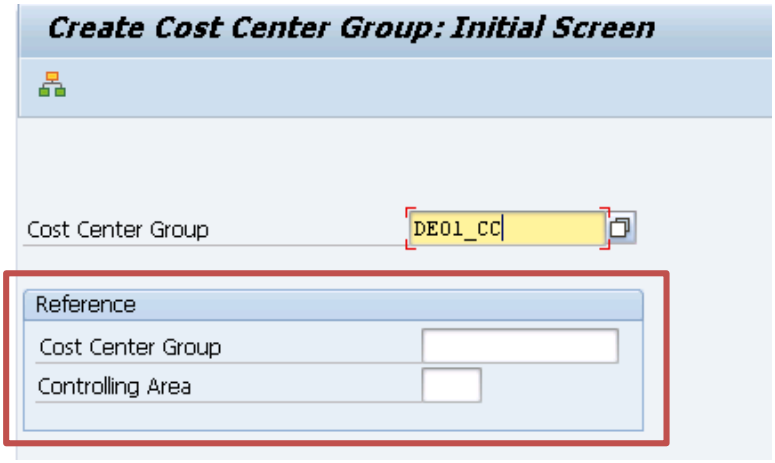
6. KS03 - Display cost center

   The authorization object for displaying cost centers is **K_CSKS**. This authorization object protects the cost centers in master data maintenance for Cost Center Accounting.

Authorization Object	Description	Fields	Values	Table	Role Type
K_CSKS	CO-CCA: Cost Center Master	ACTVT: Activity	03 – Role for displaying the cost center	N/A	Organizational Role
		KOSTL: Cost Center	Depends on the enterprise	CSKS	
		KOKRS: Controlling Area (that belongs to the Cost Center)	Depends on the enterprise		

7. KSH1 - Create cost center group

   The authorization object for creating cost center groups is **K_CSKS_SET**. This authorization object protects the maintenance of cost centers groups in Cost Center Accounting.



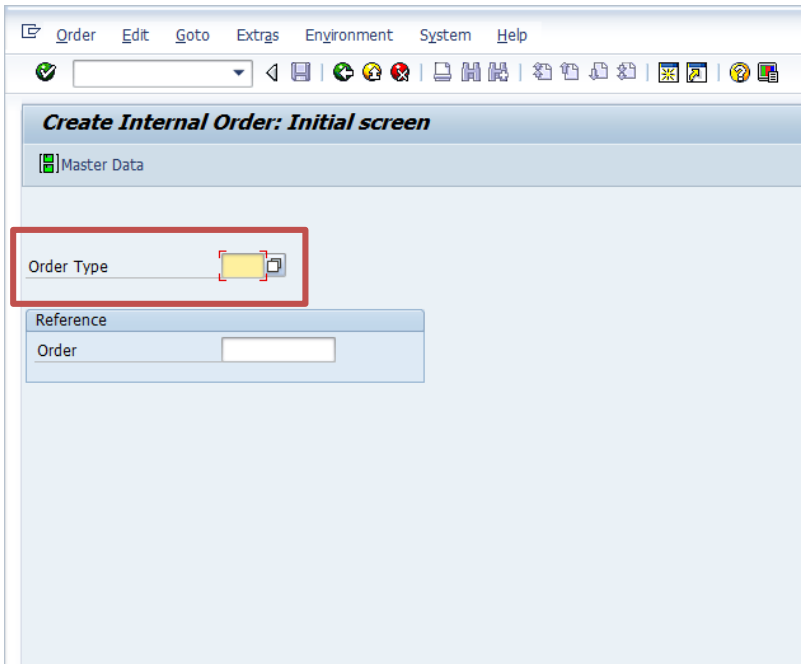
Authorization Object	Description	Fields	Values	Table	Role Type
K_CSKS_SET	CO-CCA: Cost Center Groups	ACTVT: Activity	01 – Role for creating the cost center group	N/A	Organizational Role
		KOKRS: Controlling Area (that belongs to the Cost Center)	Depends on the enterprise	CSKS	

Other activity values are 02 – Change and 03 – Display.

8. KO01 - Create internal order

The authorization object for creating internal orders is **K_ORDER**. This authorization object issues access for the following actions: maintenance of order master data, manual order planning, budgeting of orders, actions in the information systems, and also for an area of responsibility in Overhead Cost Controlling (CO-OM area of responsibility).

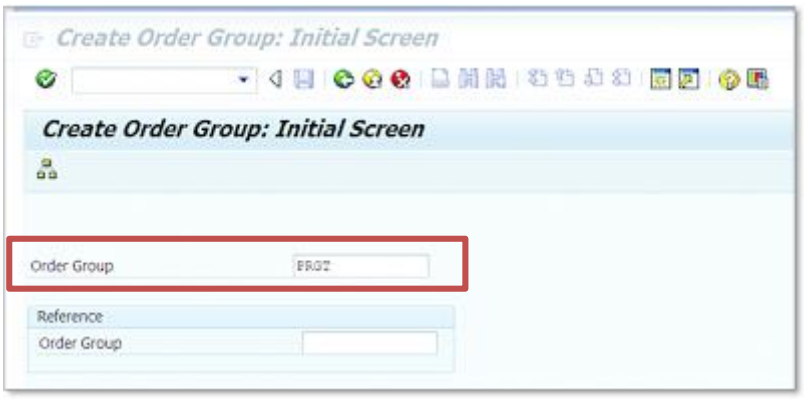
- If there is a cost center responsible for the order, the CO-OM area can include the order, the responsible cost center or a node in the standard hierarchy of the Cost Center Accounting.
- If there is no responsible cost center, the CO-OM area of responsibility applies only to the order.



Authorization Object	Description	Fields	Values	Table	Role Type
K_ORDER	CO-CCA: Cost Element Master	AUFART: Order Type	Depends on the enterprise	T0030	Organizational Role
		AUTHPHASE: Internal Order Authorization – Authorization Phase	Depends on the enterprise	N/A	
		CO_ACTION: Actions for CO-OM Authorization Check	Depends on the enterprise		
		KSTAR: Cost Element	Depends on the enterprise	CSKB	
		RESPAREA: CO-OM Responsibility Area	Depends on the enterprise		

9. KOH1 - Create internal order group

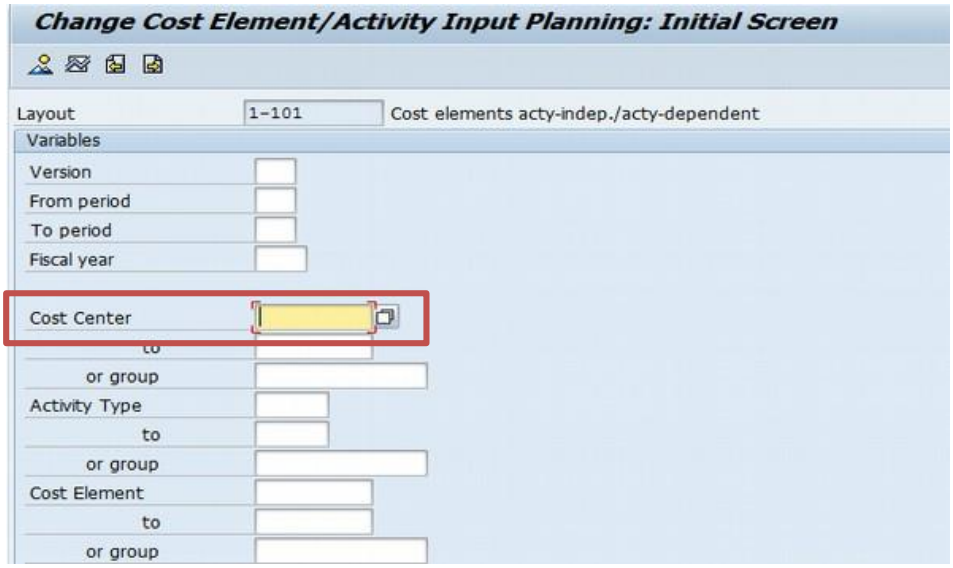
   The authorization object for creating internal orders is **K_AUFK_SET**. This authorization object protects the maintenance of the order groups for internal orders.



Authorization Object	Description	Fields	Values	Role Type
K_AUFK_SET	CO-OPA: Order Groups	ACTVT: Activity	01 – Role for creating the internal order group	Functional Role
		HNAME: Group Name	Depends on the enterprise	

10. KP26 - Change activity type/price planning on cost center

    The authorization object for changing activity planning is **K_CSKS_PLA**. This authorization object protects cost centers in planning for Cost Center Accounting.

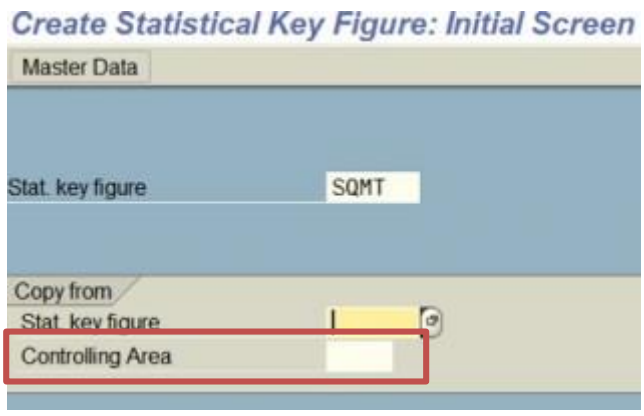


Authorization Object	Description	Fields	Values	Table	Role Type
K_CSKS_PLA	CO-CCA: Cost Center Planning	ACTVT: Activity	02 – Role for changing activity type/price planning	N/A	Organizational Role
		KOSTL: Cost Center	Depends on the enterprise	CSKS	
		KOKRS: Controlling Area	Depends on the enterprise		

Other activity value is 03 – Display.

11. KK01 - Create statistical figure

The authorization object for changing activity planning is **K_KA03**. This authorization object protects cost centers in planning for Cost Center Accounting.



Authorization Object	Description	Fields	Values	Table	Role Type
K_KA03	CO-CCA: Statistical Key Figures	ACTVT: Activity	02 – Role for creating or changing statistical figures	N/A	Organizational Role
		KOKRS: Controlling Area	Depends on the enterprise	CSKS	

12. KBH1 - Create statistical key figure group

The authorization object for changing activity planning is **K_KA03_SET**. This authorization object protects the maintenance of statistical key figure groups.

Authorization Object	Description	Fields	Values	Table	Role Type
K_KA03_SET	CO-CCA: Statistical Key Figure Groups	ACTVT: Activity	02 – Role for creating or changing statistical key figure groups	N/A	Organizational Role
		KOKRS: Controlling Area	Depends on the enterprise	CSKS	

13. KSCF - Carry forward cost center commitment

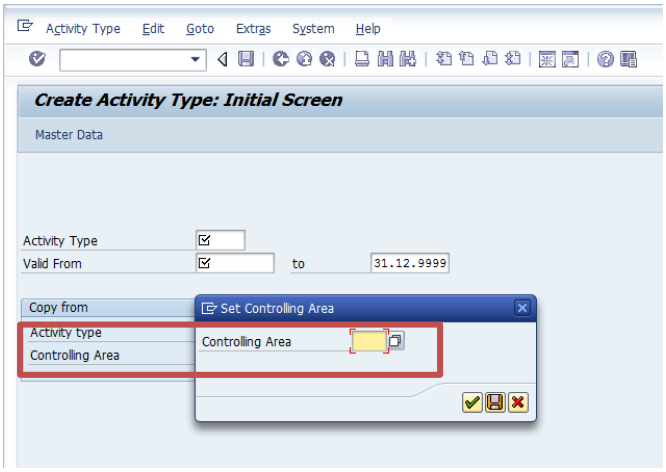
The authorization object for carrying forward cost center commitment is **K_VRGNG**. This authorization object protects manual actual cost postings, and allocations of planned and actual costs, which change the data of a whole controlling area (or larger areas).

Authorization Object	Description	Fields	Values	Table	Role Type
K_VRGNG	CO: Bus. Trans., Actual Postings and Plan/Act. Allocations	ACTVT: Activity	48 – Role for carrying forward cost center commitment	N/A	Organizational Role
		CO_VRGNG: CO Business Transaction	Depends on the enterprise	N/A	
		KOKRS: Controlling Area	Depends on the enterprise	CSKS	

Other activity values are 03 – Display, 06 – Cancel and 16 – Create.

14. KL01 - Create activity type

The authorization object for creating activity types is **K_CSLA**. This authorization object protects activity types in the processing of master data maintenance.



Authorization Object	Description	Fields	Values	Table	Role Type
K_CSLA	CO-CCA: Activity Types Master	ACTVT: Activity	01 – Role for creating activity types	N/A	Organizational Role
		KOKRS: Controlling Area	Depends on the enterprise	CSKS	

15. KLH1 - Create activity type group

16. The authorization object for creating activity types is **K_CSLA_SET**. This authorization object protects the maintenance of the activity type groups.

Authorization Object	Description	Fields	Values	Table	Role Type
K_CSLA_SET	CO-CCA: Activity Type Groups	ACTVT: Activity	01 – Role for creating activity types	N/A	Organizational Role
		KOKRS: Controlling Area	Depends on the enterprise	CSKS	

17. KB11N - Enter manual repostings of costs

The authorization object for carrying forward cost center commitment is **K_VRGNG**. This authorization object protects manual actual cost postings, and allocations of planned and actual costs, which change the data of a whole controlling area (or larger areas).

Authorization Object	Description	Fields	Values	Table	Role Type
K_VRGNG	CO: Bus. Trans., Actual Postings and Plan/Act. Allocations	ACTVT: Activity	16 – Role for entering manual repostings of costs	N/A	Organizational Role
		CO_VRGNG: CO Business Transaction	Depends on the enterprise	N/A	
		KOKRS: Controlling Area	Depends on the enterprise	CSKS	

Other activity values are 03 – Display, 06 – Cancel and 16 – Create.

18. KO88 - Actual settlement: Order

The authorization object for carrying forward cost center commitment is **K_VRGNG**. This authorization object protects manual actual cost postings, and allocations of planned and actual costs, which change the data of a whole controlling area (or larger areas).

Authorization Object	Description	Fields	Values	Table	Role Type
K_VRGNG	CO: Bus. Trans., Actual Postings and Plan/Act. Allocations	ACTVT: Activity	48 – Role for actual settlement	N/A	Organizational Role
		CO_VRGNG: CO Business Transaction	Depends on the enterprise	N/A	
		KOKRS: Controlling Area	Depends on the enterprise	CSKS	

Other activity values are 03 – Display, 06 – Cancel and 16 – Create.

19. S_ALR_87005757 - Create distribution assessment cycle

The authorization object for carrying forward cost center commitment is **K_VRGNG**. This authorization object protects manual actual cost postings, and allocations of planned and actual costs, which change the data of a whole controlling area (or larger areas).

Authorization Object	Description	Fields	Values	Table	Role Type
K_VRGNG	CO: Bus. Trans., Actual Postings and Plan/Act. Allocations	ACTVT: Activity	01 – Role for creating distribution assessment cycle	N/A	Organizational Role
		CO_VRGNG: CO Business Transaction	Depends on the enterprise	N/A	
		KOKRS: Controlling Area	Depends on the enterprise	CSKS	

Other activity values are 03 – Display, 06 – Cancel and 16 – Create.

20. KSU1 - Create actual assessment

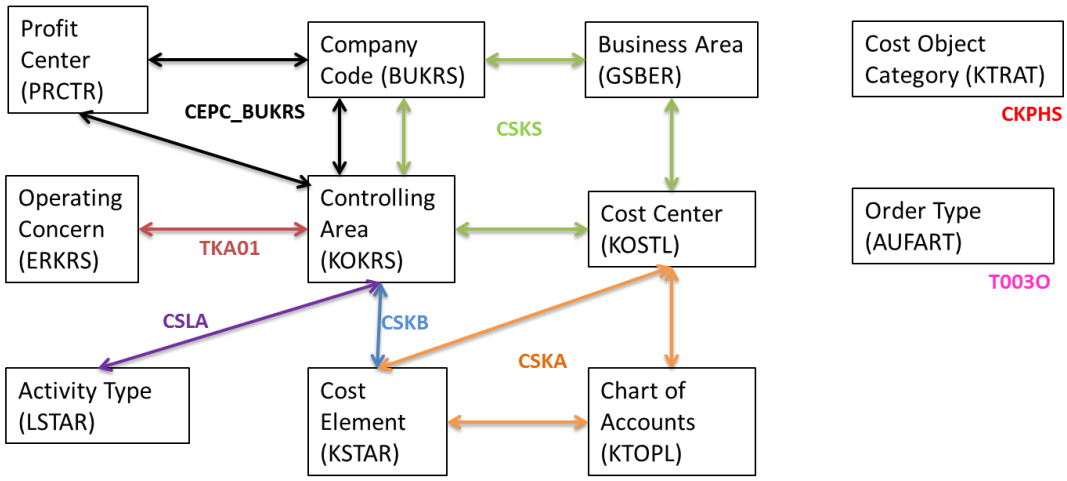
The authorization object for carrying forward cost center commitment is **K_VRGNG**. This authorization object protects manual actual cost postings, and allocations of planned and actual costs, which change the data of a whole controlling area (or larger areas).

Authorization Object	Description	Fields	Values	Table	Role Type
K_VRGNG	CO: Bus. Trans., Actual Postings and Plan/Act. Allocations	ACTVT: Activity	01 – Role for creating actual assessment	N/A	Organizational Role
		CO_VRGNG: CO Business Transaction	Depends on the enterprise	N/A	
		KOKRS: Controlling Area	Depends on the enterprise	CSKS	

Other activity values are 03 – Display, 06 – Cancel and 16 – Create.

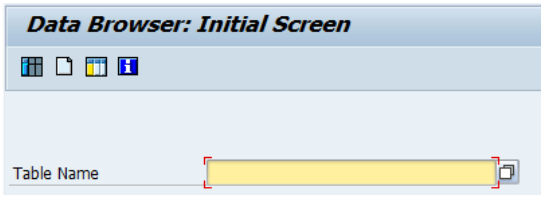
Controlling Tables

The tables that relate Controlling fields are the following:

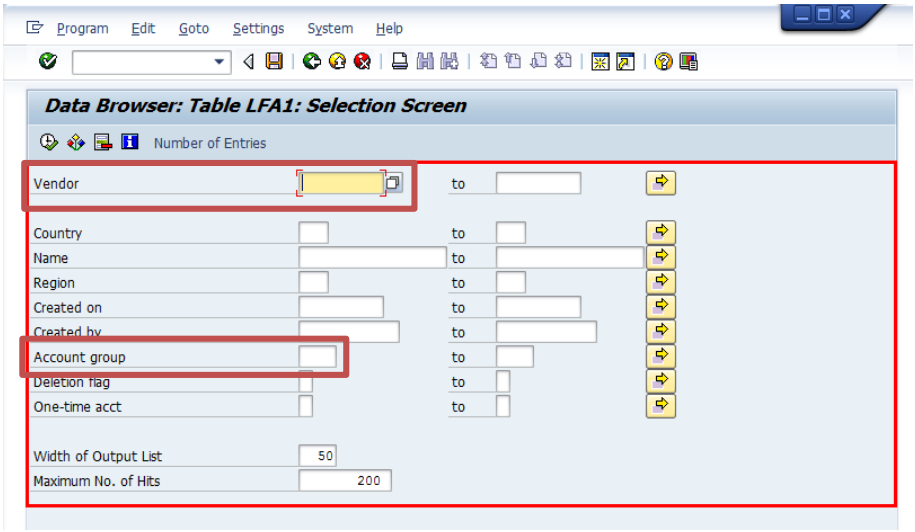


Every arrow (p.e CSLA) defines the name of the table that links two different fields (LSTAR and KOKRS, in this case).

In order to search a table in SAP to display all results related to that specific data, SE16 is a transaction where we can browse any table.

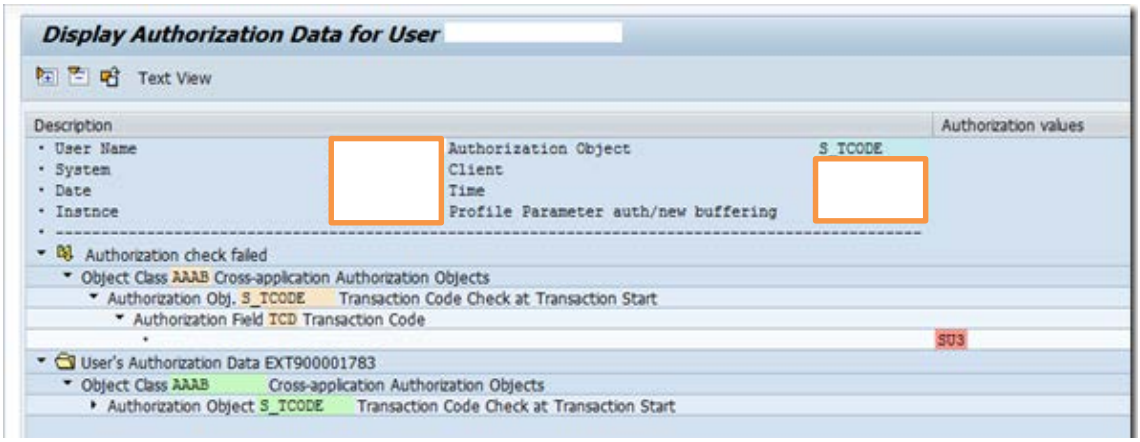


We type the name of the table, e.g. LFA1 (Vendor Master) and there is a list of all the fields that are associated to the table LFA1, such as MANDT (Vendor) and KTOKK (Vendor account group).



12 Appendix C: Solutions for Users' Access Denial

12.1.1 Solution to access: SU53



The image above represents an example of transaction SU53. In this case, the authorization object that is missing is S_TCODE for the value SU3, which means that this user does not have access to this transaction.

The solution to authorize this user should be:

1. Check if this transaction is included in any of the **existent roles** in the system
   - 1.1.1. **YES:** In that case, check to what **department** this user works for
     Then, check if the people working in that department have this role
     a. **YES:** Assign this role too to this user
     b. **NO:** Contact this user and his/her managers to understand why this user needs access to this transaction, and then, contact Internal Control to check if this complies with SoD matrix and not pose any risk for the company.
   - 1.1.2. **NO:** As this transaction is not included in any of the existing roles, consultants should check what this transaction is used for, and who should have access to this transaction.
     To analyze what this transaction is used for, we should trace this transaction, and verify the authorization objects that it checks.
     Check if the functionality of this transaction is equivalent to other functions in the system
     a. **YES:** Then, security consultants could include this transaction in a role with similar functions, and continue with step 1.1.1.

b. **NO:** Analyze it in depth detail and if necessary, contact the developer of this transaction to comprehend its functionality, and ask him/her who requested its development.

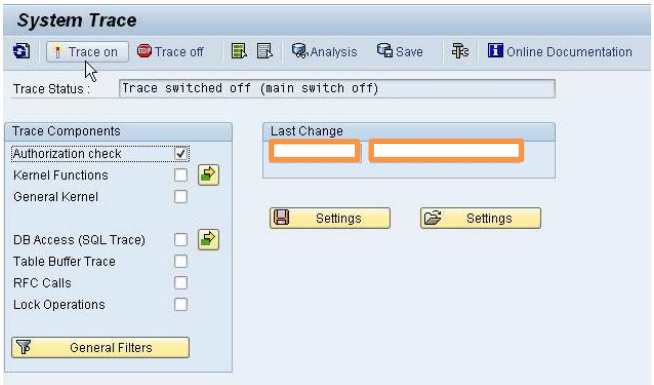
Once this is done, security consultants could:

1. **If it does not pose any risk and the transaction development is correct:** Create a new role for this transaction, or include it in any of the existent roles that this user has.
2. **If this transaction is not correct and risky:** Contact Internal Control about this problem and analyze it with the managers who requested its use.

If the authorization object that appears on the SU53 screenshot is different than S_TCODE, it will mean that there are some authorization objects that are being checked during its process and the user has not access to them. This can either mean that there are some functionalities in the transaction that have not been authorized and, thus, they are disabled for the user; or it can mean that from this transaction there is a direct jump query to other transaction(s) and the user has not been authorized for this new transaction(s).

12.1.2 Solution to access: ST01

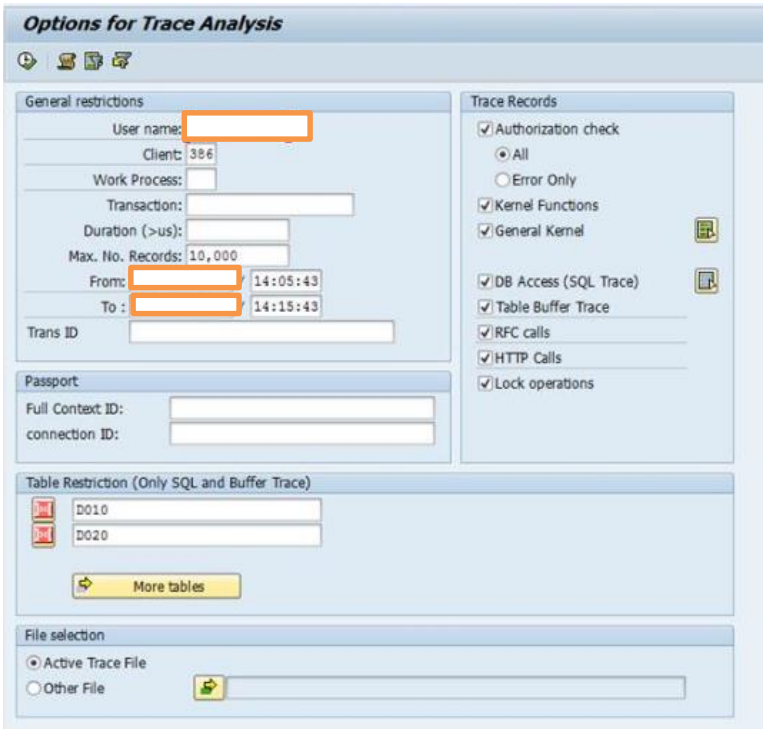
When SU53 is not enough explanatory, consultants can use the transaction ST01 for tracing the whole transaction and see every authorization object that is being checked.



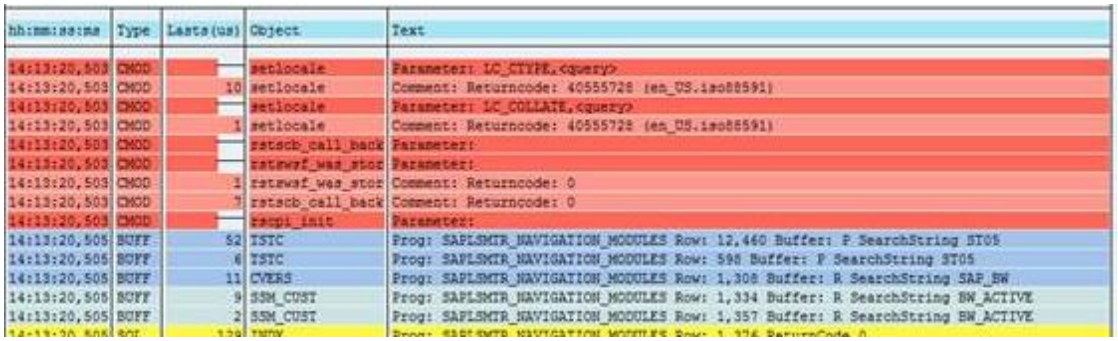
To activate the trace, we enter in ST01 and then, select Authorization check and click in 'Trace on'.

At this moment, the system starts tracing every authorization object that the system checks in this session from the user we are connected.

Once we have executed the whole process of the transaction until we had the authorization check denial, we open again the transaction ST01 and select the schedule where this process was executed.



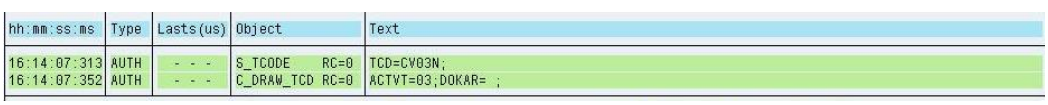
The result of ST01 when a user did not have all authorizations needed looks like this:



Each of the lines listed indicate the authorization objects that are being checked by the system when executing the program coding of a transaction. Colors determine whether the user has access or not.

	WARNING: Determine which authorization objects are missing in the user privileges.
	Show that system is searching for information in the program
	Some additional values are missing in its configuration
	User has access to these authorization objects

However, this is the result when the user has access to the authorization objects checked.



REFERENCES

ABC News. (2007, October 25). *TJX data breach may involve 94 million credit cards.* Retrieved from ABC News: http://abcnews.go.com/Technology/story?id=3773782&page=1

Albrecht, S. H. (1984). *Deterring fraud: the internal auditor's perspective.* Institute of Internal Auditors Research Foundation.

Análisis Global. (2009, January 21). *El caso Madoff: ¿Quién era? ¿Cómo maquinó su estafa? ¿Por qué nadie lo detectó? | Análisis global.* Retrieved from Análisis Global: https://analisisglobal.wordpress.com/2009/01/21/el-caso-madoff-%C2%BFquien-era-%C2%BFcomo-maquino-su-estafa-%C2%BFpor-que-nadie-lo-detecto/

Barca, A. J. (2009, February 1). *El hombre de los 5.000 millones | Edición impresa | EL PAÍS.* Retrieved from EL PAÍS S.L.: http://elpais.com/diario/2009/02/01/economia/1233442804_850215.html

BDO Consulting (BDOC). (2010). *BDO Ac'sense 2010 self-study course - Focus on Fraud: The Series Continues.* Retrieved from BDO USA, LLP | Accounting, Tax, Audit & Consulting Services: https://www.bdo.com./acsense/events/Focus%20on%20Fraud%20-%20Lessons%20Learned.aspx

Benito, M. (2012, October 27). *Jérôme Kerviel, el trader de origen humilde que creyó ser Dios. Noticias de Economía.* Retrieved from El Confidencial: http://www.elconfidencial.com/economia/2012-10-27/jerome-kerviel-el-trader-de-origen-humilde-que-creyo-ser-dios_423632/

Bhattacharjee, A. (2014, April 29). *SAP FI - All About Financial Accounting and Transactions.* Retrieved from Udemy Blog: https://blog.udemy.com/sap-fi/

Bloomberg. (2009, July 7). *Lessons from the Data Breach at Heartland.* Retrieved from Bloomberg: http://www.bloomberg.com/news/articles/2009-07-06/lessons-from-the-data-breach-at-heartlandbusinessweek-business-news-stock-market-and-financial-advice

Burnson, F. (2015). *Enterprise Resource Planning Software Buyer Report - 2015.* Retrieved from Software Advice: http://www.softwareadvice.com/resources/erp-buyer-report-2015/

Business Insider. (2014, May 27). *Cyber Thieves Took Data On 145 Million eBay Customers By Hacking 3 Corporate Employees.* Retrieved from Business Insider: http://www.businessinsider.com/cyber-thieves-took-data-on-145-million-ebay-customers-by-hacking-3-corporate-employees-2014-5

Calvo, P. (2013, December 11). *Bernard Madoff: cinco años del escándalo que destapó las vergüenzas de las finanzas. Noticias de Mercados.* Retrieved from El Confidencial: http://www.elconfidencial.com/mercados/2013-12-11/bernard-madoff-cinco-anos-del-escandalo-que-destapo-las-verguenzas-de-las-finanzas_64789/

CISCO & BT. (2016). *Las amenazas a la seguridad en cifras.* Retrieved from CISCO & BT: http://www.losmayoresciberataques.com/14-empresas-hundidas-por-fallos-de-seguridad

COMODO. (2013, October 15). *The Heartland Breach: A Cautionary Tale for E-Commerce.* Retrieved from COMODO: https://blog.comodo.com/e-commerce/the-heartland-breach-a-cautionary-tale-for-e-commerce/

Consultoría SAP. (2016, May 13). *Perfil SAP_ALL con solo visualización.* Retrieved from Consultoría SAP: http://foros.consultoria-sap.com/t/perfil-sap-all-con-solo-visualizacion/6220/2

DataWarehouse4u. (2010). *OLTP vs. OLAP.* Retrieved from Data Warehouse 4u Website: http://datawarehouse4u.info/OLTP-vs-OLAP.html

Deloitte, R. M. (2014, October 15). *Risk Technology Strategy, Selection and Implementation.* Retrieved from SlideShare: http://www.slideshare.net/RMIA_events/risk-technology-strategy-selection-and-implementation

Dorminey, J. F.-J. (2011). The evolution of fraud theory. *American Accounting Association Annual Meeting* (pp. 1-58). Denver: Accounting Education. doi:http://dx.doi.org/10.2308/iace-50131

El Confidencial. (2016, April 21). *Fernández de Sousa 'revivió' su offshore de Islas Vírgenes cuando estalló Pescanova.* Retrieved from El Confidencial: http://www.elconfidencial.com/economia/papeles-panama/2016-04-21/fernandez-de-sousa-pescanova-papeles-panama-papers-offshore-islas-virgenes-mossack-fonseca_1183335/

Experian. (2014, March 30). *The Facts on Court Ventures and Experian.* Retrieved from Experian: http://www.experian.com/blogs/news/2014/03/30/court-ventures/

EY. (2010, May). *Insights on governance, risk and compliance.* Retrieved from EY: http://www.ey.com/Publication/vwLUAssets/EY_Segregation_of_duties/$FILE/EY_Segregation_of_duties.pdf

Finkle, J. (2016, April 25). *Bangladesh Bank hackers compromised SWIFT software, warning issued.* Retrieved from Reuters: http://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR

Garmendia, I. (2012, March 12). *¿Qué es SAP Finanzas? (SAP FI).* Retrieved from Oreka i.t. corporate balance: http://orekait.com/blog/%C2%BFque-es-sap-finanzas-sap-fi/

Global Cybersec. (2016, May 27). *Grupo de Hackers "Lazarus" de Corea del Norte vinculados con Swift.* Retrieved from Global Cybersec: http://www.globalcybersec.com/reader.php?p=1744

Hani, M. (2013, April 20). *SAP Controlling Overview.* Retrieved from SlideShare - A LinkedIn Corporation: http://es.slideshare.net/mohamedhani89/sap-controlling-overview

IBM. (2015, December 21). *Average cost per compromised record hits $154.* Retrieved from IBM Cost of Data Breach: http://www.ibmcostofdatabreach.com/

infoLibre. (2016, April 21). *El expresidente de Pescanova tuvo una sociedad 'offshore' creada a través de Mossack Fonseca.* Retrieved from infoLibre: http://www.infolibre.es/noticias/politica/2016/04/21/el_expresidente_pescanova_tuvo_una_sociedad_offshore_creada_traves_mossack_fonseca_48557_1012.html

Integrc. (2015). *What is SAP GRC?* Retrieved from Integrc: http://www.integrc.com/overview-what-is-sap-grc-integrc

ISACA. (2012). *COBIT 5 for Information Security.* Rolling Measdows, IL, USA.

Kassem, R., & Highson, A. (2012). The new fraud triangle model. *Journal of Emerging Trends in Economics and Management Sciences, 3*(3), 191-195.

Kennedy, K. (2012). *An Analysis of Fraud: Causes, Prevention and Notable Cases.* Durham, NH, USA: University of New Hampshire.

Knop, D. (2016, April 5). *Associate fraud: who they are and why they do it.* Retrieved from UMass Boston Blog Network: http://blog.umb.com/associate-fraud/

Krebs on Security. (2015, July 21). *Experian Hit With Class Action Over ID Theft Service.* Retrieved from Krebs on Security: In-depth security news and investigation: http://krebsonsecurity.com/2015/07/experian-hit-with-class-action-over-id-theft-service/

La Nación | El Mundo. (2002, June 15). *Enron: la auditoria Andersen, declarada culpable por obstruir el caso.* Retrieved from LA NACION | El Mundo: http://www.lanacion.com.ar/405671-enron-la-auditora-andersen-declarada-culpable-por-obstruir-el-caso

La Voz de Galicia. (2015, November 28). *La CNMV multa a Pescanova con 450.000 euros y a su expresidente con 225.000 euros.* Retrieved from La Voz de Galicia: http://www.lavozdegalicia.es/noticia/economia/2015/11/28/cnmv-multa-pescanova-450000-euros-expresidente-225000-euros/00031448728437001373745.htm

Lingard UK. (n.d.). *SAP Software R/2 and R/3.* Retrieved from Lingard UK: http://www.lingard.co.uk/jonathan/sap.htm

Lord, N. (2015, September 28). *The History of Data Breaches.* Retrieved from Digital Guardian: https://digitalguardian.com/blog/history-data-breaches

Lormel, D. (2012). *The Fraud Diamond.* Retrieved from ACAMS Today: http://www.acamstoday.org/can-you-think-like-a-bad-guy

McNally, J. S., & CPA. (2013). *The 2013 COSO Framework & SOX Compliance.* ima | The Association of Accountants and Professionals in Business.

Mora, M. (2014, March 19). *El Supremo confirma la pena de cárcel para Jérôme Kerviel | Economía | EL PAÍS.* Retrieved from EDICIONES EL PAÍS S.L.: http://economia.elpais.com/economia/2014/03/19/actualidad/1395251705_606783.html

NBC News. (2005, August 8). *Ex-AOL worker who stole e-mail list sentenced.* Retrieved from NBC News: http://www.nbcnews.com/id/8985989/ns/technology_and_science-security/t/ex-aol-worker-who-stole-e-mail-list-sentenced/#.V2M9s_mLTIU

NBC News. (2007, October 24). *TJX breach could top 94 million accounts.* Retrieved from NBC News: http://www.nbcnews.com/id/21454847/ns/technology_and_science-security/t/tjx-breach-could-top-million-accounts/#.V2Pu5PmLTIU

Opinno. (2015, September 30). *Innovation in Communication: Renovate or Die.* Retrieved from Opinno - We deliver impact through innovation: http://www.opinno.com/en/content/innovation-communication-renovate-or-die?language=en

PCADvisor. (2012, February 16). *The 15 worst data security breaches of the 21st Century.* Retrieved from PCADvisor: http://www.pcadvisor.co.uk/news/security/15-worst-data-security-breaches-of-21st-century-3338236/

Pepitone, J., & Remizowski, L. (2012, April 2). *Massive credit card data breach involves all major brands.* Retrieved from CNN Money - The Cybercrime Economy: http://money.cnn.com/2012/03/30/technology/credit-card-data-breach/index.htm

Project Management Institute (PMI). (2013). PMBOK® Guide and Standards. In P. M. (PMI), *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)* (p. 459). Project Management Institute.

Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, S., Salamasick, M., & Riddle, C. (2013). *Internal Auditing: Assurance & Advisory Services.* The IIA Research Foundation.

Reuters. (2013, April 16). *Accounting scandal deepens at Spain's Pescanova.* Retrieved from Reuters | Markets: http://www.reuters.com/article/pescanova-idUSL5N0D32HJ20130416

Reuters. (2014, May 21). *EBay asks 145 million users to change passwords after cyber attack.* Retrieved from Reuters: http://www.reuters.com/article/us-ebay-password-idUSBREA4K0B420140521

SAP. (2014, April 4). *IT Simplification with the SAP HANA Platform.* Retrieved from SAP Software Solutions | Technology & Applications: http://www.sap.com/bin/sapcom/en_us/downloadasset.2014-04-apr-09-16.it-simplification-with-the-sap-hana-platform-uncover-value-and-realize-the-breakthroughs-that-drive-success-pdf.html

SAP Corporation. (n.d.). *The Segregation of Duties Concept.* Retrieved from SAP GRC Access Control: https://help.sap.com/saphelp_grcac53/helpdata/en/17/76b1e9bb29435582eb8ef3366112c6/content.htm

SAP GRC. (2007). GRC Compliance Week.

SAP Security Analyst. (2014). *SU25 (Maintain Check Indicators).* Retrieved from SAP Security Analyst: http://sapsecurityanalyst.com/WP/general-disclaimer/su24-concept-in-sap

Sarbanes, P. (2002, July). Sarbanes-Oxley Act of 2002. *The Public Company Accounting Reform and Investor Protection Act. Washington DC: US Congress.*

Silverstein, K. (2013, May 10). *Enron's Painful Lessons.* Retrieved from EnergyBiz for Leaders in the Global Power Industry: http://www.energybiz.com/article/13/05/enrons-painful-lessons

Tarantino, A., & Cernauskas, D. (2009). *Risk Management in Finance: Six Sigma and other Next Generation Techniques.* Hoboken, New Jersey; Canada: John Wiley & Sons, Inc.

The City of London Police. (2016, March 10). *City of London Police reveals for the first time who is being targeted by cyber criminals.* Retrieved from The City of London Police Website: https://www.cityoflondon.police.uk/news-and-appeals/Pages/City-of-London-Police-reveals-for-the-first-time-who-is-being-targeted-by-cyber-criminals-.aspx

The New York Times. (2002, October 17). *Arthur Andersen Is Fined $500,000 - NYTimes.com.* Retrieved from The New York Times: http://www.nytimes.com/2002/10/17/business/arthur-andersen-is-fined-500000.html

The New York Times. (2007, October 24). *Banks claim credit card breach affected 94 million accounts.* Retrieved from The New York Times: http://www.nytimes.com/2007/10/24/technology/24iht-hack.1.8029174.html?_r=0

The Resource Group. (2015). *History of Enterprise Resource Planning, at a Glance.* Retrieved from The Resource Group: http://www.resgroup.com/accounting-software-history-enterprise-resource-planning-glance

The SAP Expert Base . (2000). *SAP R/3 Industry Solutions.* Retrieved from The SAP Expert Base : http://www.sap-expertbase.nl/

The Washington Post. (2004, June 24). *AOL Employee Charged in Theft Of Screen Names.* Retrieved from The Washington Post: http://www.washingtonpost.com/wp-dyn/articles/A860-2004Jun23.html

The Washington Post. (2014, May 21). *eBay asks 145 million users to change passwords after data breach.* Retrieved from The Washington Post: https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/

Turban, E., Sharda, R., Delen, D., & King, D. (2010). *Business Intelligence: A Managerial Approach.* Prentice Hall.

Universia Knowledge@Wharton. (2003, January 7). *¿Qué falló en WorldCom? - Universia Knowledge@Wharton.* Retrieved from Universia Knowledge@Wharton: http://www.knowledgeatwharton.com.es/article/que-fallo-en-worldcom/

Wells, J. (2005). Fraud Triangle. In J. Wells, *Principles of fraud examination.* Hoboken, New York: John Wiley and Sons.

Wells, J. (2005). Fraud Triangle. In J. Wells, *Principles of fraud examination.* Hoboken, New York: John Wiley and Sons.

WIRED. (2004, June 23). *AOL Worker Sells 92 Million Names.* Retrieved from WIRED Politics: Security: http://archive.wired.com/politics/security/news/2004/06/63970