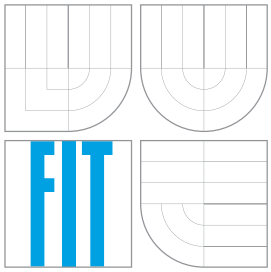
BRNO UNIVERSITY OF TECHNOLOGY
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ



FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

APPLICATION FOR RISK MANAGEMENT REPORTING IN SAP

APLIKACE PRO REPORTOVÁNÍ SPRÁVY RIZIK V SYSTÉMU SAP

MASTER'S THESIS
DIPLOMOVÁ PRÁCE

AUTHOR — Bc. MICHAL UHLÍŘ
AUTOR PRÁCE

SUPERVISOR — doc. Ing. JAROSLAV ZENDULKA, CSc.
VEDOUCÍ PRÁCE

BRNO 2016

Master Thesis Specification/18963/2015/xuhlir14

Brno University of Technology - Faculty of Information Technology

Department of Information Systems | Academic year 2015/2016

Master Thesis Specification

For: **Uhlíř Michal, Bc.**
Branch of study: Information Systems
Title: **Application for Risk Management Reporting in SAP**
Category: Databases

Instructions for project work:

1. Get acquainted with risk management in companies.
2. Study new SAP technologies to support reporting in web browser.
3. Analyze the database structure of SAP GRC module for risk management.
4. Optimize the database structure for SAP CDS technology.
5. Create unit tests to validate the opimized database structure.
6. By prior arrangement with your supervisor, develop an application for risk management reporting using the optimized structure in SAP HANA.
7. Discuss the achieved results and possible future work.

Basic references:

- Schöler, S., Zink, O.: SAP governance, risk and compliance. 1st ed. Boston: Galileo Press, 2009. ISBN 9781592291915.
- Wood, J., Hof, R.: Getting started with SAP HANA cloud platform. 1st edition. Boston: Rheinwerk Publishing, 2015, 519 pages. ISBN 1493210238.
- Platner, H.: A Course in In-Memory Data Management. Springer, 2013. ISBN 978-3-642-36523-2.

Requirements for the semestral defense:

- The first 3 items.

Detailed formal specifications can be found at http://www.fit.vutbr.cz/info/szz/

The Master Thesis must define its purpose, describe a current state of the art, introduce the theoretical and technical background relevant to the problems solved, and specify what parts have been used from earlier projects or have been taken over from other sources.

Each student will hand-in printed as well as electronic versions of the technical report, an electronic version of the complete program documentation, program source files, and a functional hardware prototype sample if desired. The information in electronic form will be stored on a standard non-rewritable medium (CD-R, DVD-R, etc.) in formats common at the FIT. In order to allow regular handling, the medium will be securely attached to the printed report.

Supervisor: **Zendulka Jaroslav, doc. Ing., CSc.**, DIFS FIT BUT
Consultant: Orság Martin, Ing., SAP
Beginning of work: November 1, 2015
Date of delivery: May 25, 2016

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav informačních systémů
612 66 Brno, Božetěchova 2

L.S.

Dušan Kolář
Associate Professor and Head of Department

Abstract

The main prupose of this thesis is to develop an application for Risk Management Reporting using the latest technologies provided by SAP. The first part of the paper is desrcibing the theory of Governance, Risk and Compliance Management. It is analyzing the definition of the concept and mentioning key challenges that companies need to deal with today. Then the most complex GRC software solutions are listed and compared to each other. After the relevant SAP technologies are introduced, the development of the application itself is described. Firstly, the data structure of the standard solution was analyzed, then new data structure was designed and validated. The developed application is able to fetch the correct data from the database and display them accordingly.

Abstrakt

Hlavním cílem této práce je vyvinout aplikaci sloužící pro reportování správy rizik za použití nejnovějších technologií, které nabízí firma SAP. V první části je nastíněn koncept problematiky správy rizik, jsou vysvětleny klíčové pojmy a zmíněny některé problémy z této oblasti, se kterými se společnosti v dnešní době potýkají. Dále jsou vyjmenována a srovnána některá z komplexních softwarových řešení, které jsou momentálně dostupné na trhu. Práce pokračuje popisem technologií, které jsou využity při tvorbě výsledné aplikace. Proces vývoje zahrnoval analýzu stávajícího datového modelu, tvorbu nové datové struktury a její validaci a návrh samotného uživatelského prostředí pro zobrazování těchto dat. Výsledná aplikace umožňuje získávat správná data z databáze a zobrazovat je odpovídajícím způsobem.

Keywords

Risk Management, SOX, SAP, CDS, APF, SAP Fiori, SAPUI5

Klíčová slova

Správa rizik, SOX, SAP, CDS, APF, SAP Fiori, SAPUI5

Reference

UHLÍŘ, Michal. *Application for Risk Management Reporting in SAP*. Brno, 2016. Master's thesis. Brno University of Technology, Faculty of Information Technology. Supervisor Zendulka Jaroslav.

Application for Risk Management Reporting in SAP

Declaration

I declare that this project in my own work that has been created under the supervision of doc. Ing. Jaroslav Zendulka, CSc., and all sources and literature that I have used during elaboration of the project are correctly cited with complete reference to the corresponding sources.

.....
Michal Uhlíř
May 25, 2016

Acknowledgements

I would like to thank to my supervisor Doc. Ing. Jaroslav Zendulka, CSc., who supported me throughout my work on this project, you have been a tremendous mentor for me. I would especially like to thank to employees of SAP for their time spent with me discussing SAP Hana, SAP Fiori Development and Governance, Risk and Compliance Management. My consultants Martin Orsag and Daniel Welzbacher. Furthermore I would like to thank my school mates, parents and girlfriend for their support during my studies.

Contents

Chapter 1

Introduction

Governance, Risk and Compliance Management (GRC) became an important topic for all bigger companies today. Above all the recent financial crisis verified the governance and risk management of corporations and proved that the system is highly deficient. It increased the focus on this area from inside the companies as well as from external stakeholders. The demand for any systematic approach and complex solution is therefore enormous.

The main goal of this thesis is to analyze new technologies, which could be used for GRC reporting. As part of back-end technologies analysis, it is expected to provide simplified data structure to fetch data and provide them as a service. This service will be ready to use by front-end technologies to display the data. The output of my analysis will be a reporting application, developed using analyzed technologies. Then the summarization of advantages, disadvantages and issues I faced during the development. This summarization will be considered by SAP GRC development team before the new wave of development.

The second chapter of this thesis is describing the definition of the concept and explaining what challenges companies face and why. It is analyzing basic principles of identification, measuring, monitoring and management of risks, compliance and governance issues. By the description of the GRC processes in an organization the need for constant processing and reporting of various data is explained. GRC stakeholders therefore need centralized frameworks to integrate the data from various systems.

The third chapter is introducing the GRC software solutions that are nowadays widely used, as their complexity is able to meet high requirements of the companies. With help of these systems, organizations can analyze, monitor and manage risks and any GRC related data. SAP BusinessObjects GRC is a comprehensive set of various subsystems that create together powerful GRC tool. By using this tool companies are able to conduct internal and external audits and controls, manage access authorizations, support corporate compliance programs, monitor and manage risks, prevent any possible loss resulting from unidentified risk and perform many other related activities. Then similar solutions from Oracle, IBM and RSA are introduced.

In following two chapters some SAP back-end and front-end technologies are mentioned. Above all the technologies used for development of my application are pointed out.

In the last four chapters I am describing the development of the application. Firstly, I analyzed the current database structure of GRC solution from SAP. Based on this I set up and validated my own data model. After the back-end of the application was successfully created I designed and developed the user interface. When developing the application I encountered some challenges and technical issues that are mentioned at the end of the thesis as well.

Chapter 2

Governance, Risk and Compliance Management

This chapter provides a general overview of how dedicated risk management can help the companies to run their business better with the help of GRC. The first section offers a definition of the concept in general and explains some key terms. The second section is then mentioning Sarbanes-Oxley (SOX) law, which is a basic legal regulation dealing with GRC and which is binding all the publicly held U.S. companies. To understand the topic of GRC in a wider context, the last section is then listing and explaining some relevant terms that are being mentioned often when speaking about GRC.

2.1 Definition of concept

The main goal of GRC is to help companies to follow policies, to be compliant with the law and obligations and to prevent any potential fraud. It creates a centralized system that enables higher efficiency in running a business by tracking activities and raising alerts, when risks might appear. Companies that understand risks and are able to identify opportunities and challenges are gaining hereby a competitive advantage. GRC is therefore not only a tool for a prediction and an inspection of risks. It plays an important role in strategic decision-making as well.

GRC is often perceived to be only an instrument how to be compliant with all the legal requirements in the respective business period. This understanding is, however, incorrect and might lead to an insufficient or wrong management of risks in the company. GRC should be understood more like a process that is constantly being developed and improved. There are a lot of factors that influence this process and these need to be evaluated repeatedly. The process needs to be then adjusted so it reacts on the changes in time.

Measures to prevent financial frauds are part of GRC as well. Chief Financial Officer (CFO) is responsible for the financial flows and needs to always be sure that there are not any discrepancies in the accounting books. GRC is therefore a powerful tool for CFO that enables him or her to be always informed about the current status and react to demands from various stakeholders such as shareholders or regulators accordingly. When a company decides to implement GRC into its corporate management, new sources of information are created. As a result, processes are improved, risks are found earlier and significant savings in auditing costs are hence made.

Even though the methods of GRC are still being developed and enhanced, the concept

itself cannot guarantee that the risk of potential fraud or any adverse event is absolutely eliminated. GRC just helps to minimize the risk but cannot completely prevent it and all the stakeholders should be aware of this fact.

2.1.1 Governance and oversight

Governance is a very general term, but in the context of GRC it is understood as a concept implemented by companies to achieve their goals while being compliant with any external or internal laws and regulations. This system should also help them to avoid risks throughout the company. Governance is generally perceived to be a responsibility of the executive management of the respective company. The main function of the board or the Chief Executive Office (CEO) is to define the strategy and risk policy. They should define, how the strategy is going to be executed, what type of policies and procedures should be followed or how those policies should be communicated through the company. Governance is also defining types of checks that need to be implemented in order to monitor that the procedures and policies are being followed. Any failure of governance is then mostly attributed to insufficient or ineffective executive management oversight.

At the beginning of definition of any governance processes within a company, there have to be a plan defined. This plan is very individual for each company or particular industry. Usually a dedicated **governance office** is established as a necessary part of the organization. The creation of such an office is strongly recommended, so it is assured that risk and compliance issues is a separated topic and there are people dedicated just to it. Another functions of this office are then prevention, fraud reporting, regular reporting or training on policies and conduct. Employees from the governance office are as well responsible for documentation and they are ensuring that information is stored in accessible centralized database to be available for all employees. It is as well important that regular employees feel authorized to report when violations to policies have occurred. They should also feel empowered to discuss any identified unknown risk scenarios with the governance office that should be therefore accessible for them.

One of the most powerful tool of governance is a control. Controls contain all of the processes, actions or physical barriers that guide a person or resource to achieve a desired result. Controls can be split to three categories. **Preventative controls**, detective controls and corrective controls. Preventative controls are commonly used to prevent any identified risk scenario. They are considered to be the most effective. This effectiveness is achieved by the fact, that the preventative controls help to deter particular damaging behavior or risk. To identify, if any wrong behavior or risk scenario has occurred or occurring, **detective controls** are being used. With this controls companies can also validate that monitored processes are being executed within the given tolerance. Example of this process can be financial reporting, payments to vendors or regulatory compliance. Detective controls are very important as they give information to help a company to understand risks and compliance and to determine reactions to them in a short time. The last type of controls are **corrective controls**. They are being carried out after particular risk scenario occurred and following actions are to be undertaken.

The call for a stronger corporate governance was always a consequence following any governance failures that revealed the weaknesses and blind spots of the system. Through the history many scandals can be found that resulted in a redesign of GRC processes, setting up of new procedures and formulation of new laws and regulations. Recent financial crisis verified the corporate governance and risk management systems as such. The experts are

agreed on the fact that one of the main causes of the crisis was a weak corporate governance of huge companies with strong impact on the whole financial system. Their governance failed completely to prevent from enormous risk taking. Legal regulations and standards also turned up to be deficient. As a result Organization for Economic Co-operation and Development (OECD) issued a paper analyzing the causes of the crisis and suggesting a reevaluation of current corporate governance. [15]

2.1.2 Risk Management

Risk is commonly defined as a potential for loss. This loss can be a reaction to any event occurring inside or outside the company. Every company runs certain types of risks. Some of them are easy to identify, some are more hidden and some do not need to be revealed until a loss is caused. However, as soon as any risk is identified, it should be properly monitored, as it may have a significant influence on running the business and the influence can change with time. In general, risk in GRC is understood as a sum of all risks that the company faces.

Types of risk can be divided into four categories. **Financial risk** can be market-dependent, determined by numerous market factors, or operational, resulting from fraudulent behavior. Financial risk can arise from such areas as financial reporting, market, financial liquidity, rating, valuation and various credit risks. **Strategic risk** is related to an organization's business strategy and strategic goals. It is a possible source of loss that can arise when the company follows no successful business strategy. **Compliance risk** is then represented by exposure to legal penalties, financial drawdown and material loss that the company faces when it fails to act in accordance with regulations, laws, prescribed best practices or internal policies. Operational risk is a form of risk that summarizes the risk that the corporation undertakes when it tries to operate within a given industry or field. **Operational risk** affects directly the ability of the company to run the business and execute the strategic plan. [13]

In 2004, The Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued a paper that defines **Enterprise Risk Management** (ERM). [22] According to COSO, ERM consists of six main activites:

- Defining and aligning risk apetite and business strategy – Risk appetite is a value that is considered by executive management during decision-making, where possible alternatives need to be evaluated. Every strategic decision should be compared to the given risk apetite and followed strategy prior it is taken.
- Improving responses to risk related decisions – ERM should provide analysis that helps the company to select among alternative risk responses. It is considering risk avoidance, reduction of risk, risk sharing and risk acceptance.
- Minimizing unexpected situations and possible losses – Companies should be able to identify adverse events that could affect their business in time.
- Identifying and managing cross-enterprise risks – ERP provides an effective response to multiple risks that are affecting more parts of the organization.
- Seizing opportunities – Management is considering all potential events and is therefore able to identify opportunities and evaluate them.

- Improving deployment of capital – Complete information about all potential risks is crucial for effective assessing of capital needs and helps to allocate capital accordingly.

Although ERM is primarily a responsibility of executive management of the company, there are many others people from the organization, who are participating in the process. **Executive management** considers risk management when deciding what corporate strategies to follow and what risk is acceptable to undergo. Once executives set the strategy, they need to review the top risks and monitor key indicators to keep company objectives on track. **Risk managers** are constantly processing all the data that they are able to pull from their enterprise systems. They use centralized framework to integrate risk data from all other systems. Risk managers are strategic advisors to the business units. The last group to mention are **line of business managers**. They need centralized tools to be able to drive their performance and react to top risks to help them achieve their objectives.

ERM is a complex process where certain steps follow each other in a given order. **Risk planning** usually involves defining the rules and processes for risk assessment, choosing who should participate in the process and capturing any other prerequisites. Planning process is supposed to find risk thresholds to manage risks more effectively and strategically. Part of the planning phase is as well to ensure that risks are aligned with corporate objectives and strategy. The main goal of **risk identification and analysis** is to find the impact of the particular risk and quantify it. It is necessary to collaborate through the company to ensure that all risks are found and aggregated and their impact to the enterprise is calculated properly. When risks are determined and potential loss is identified, adequate **risk response** needs to be made. The company needs to balance the cost of opportunity and risk avoidance. Every response should be then recorded and stored in the corporate ERM application for future references. The basis of ERM is a proper **risk monitoring** of all identified risks, as their potential impact on the business can vary with time and new risks can occur. To ensure appropriate risk monitoring companies need to allocate sufficient budget to all the related activities and establish a way and a frequency of monitoring. There are many kinds of risk dashboards available that can be used to present results of monitoring in real time to managers or executives.

2.1.3 Corporate Compliance and Regulatory

Corporate compliance should guarantee that the company implemented processes and system of controls in order to ensure that the organization is following all legal or internal rules and policies and that imposed requirements are met. Compliance is not one-time action. It should be a continuous process that ensures that the compliance sustains in a long term. There are many regulations that an organization needs to face and new one are still arising. Therefore a streamlined process that manage compliance throughout the whole company should be created.

Compliance process in general consists of multiple steps. The first one is the gathering of materials. All processes and risks need to be identified and documented. Then system of controls needs to be set up. Conducted control are then evaluated, if they are really effective and if they meet the given requirements. After the controls are done and the results are evaluated, they are documented and published. Based on this, an organization is then certified. Should any issues appear during the process, the process for the improvement is defined and launched.

Globally respected standards distinguish more types of compliance. One of the basic type of compliance is a **financial compliance** that is regulated by, for example, Sarbanes-

Oxley Act described in section 2.2. It is considered to be a crime according to the law, if financial statements are deficient in certain ways. Financial compliance means compliance in areas such as segregation of duties, accuracy of all financial statements and related reports. **Regulatory compliance** is assuming that a company follows all relevant laws and regulations. **IT compliance** means that the entire internal information system infrastructure is secured and regularly tested. [14]

Controls, the main mechanism of compliance, are the means by which violations of policies or bad behavior are detected. Controls also provide companies an alert for highlighting what mechanisms are working fine and what kind of areas need to be improved. Generally, there are two types of controls. **Preventative controls** are proactive and are set up to prevent possible errors from occurring. These are, for example, segregation of duties, system of approvals, authorization concept, verifications. Segregation of duties means in praxis that the tasks and responsibilities are distributed among various people in order to prevent potential risk of error or deceptive actions. Usually, permission to approve authorizations is separated from the operational work and handling the related assets. Management is defining processes and activities and determines, which people from the organization can perform them. Limited access to the respective transactions is then granted accordingly. Furthermore, it is defined, which transactions require approvals and what the workflows are. **Detective controls** are performed after errors occurred. The main goal of a detective control is to find the cause of the error. It analyzes what happened and detects bad behavior or policy violations. Detective controls can either be manual or automated. They have a form of reviews of performance, reconciliation, inventories and audits. [24]

2.1.4 GRC Stakeholders

Understanding of the interactions between stakeholders is a key component of a successful process of GRC improvement. Key GRC stakeholders can be separated into two categories - stakeholders inside and outside the company. [25]

Outside the company, investors and shareholders have probably the most to lose from bad implementation of GRC processes. When a stock price decreases after a company reports a material violation of compliance with regulations, or an audit failure, or any other negative event that could have been foreseen before, investors are putting forward their heavy unease. Apart from investors, there are many more stakeholders from outer environment of the company, for example:

- Non-governmental organizations are setting policies that govern how business is done.
- Financial regulators are setting standards for financial reporting, such as Financial Accounting Standards Board, Bank for International Settlements, the Securities Exchange Commission and others.
- Legislative bodies are formulating laws that have to be complied with.
- Government agencies are responsible for performing laws such as OSHA, U.S. Customs, or EPA.
- Auditing firms are controlling correctness of processes and policies used for financial reporting.
- Trade organizations like World Trade Organization, NAFTA, CAFTA and many others.

Inside the company where GRC is implemented some of the following positions will be created: Chief Compliance Officer, Vice President of Compliance, Chief Risk Officer, Chief Sustainability Officer and then managers of SOX, Compliance, Risk, Trade Management etc. In some companies some of the above mentioned positions are combined together. It is generally recommended that companies should keep any organization defined for GRC as small as it can exist and work. The ideal case to implement GRC is to make compliance easy and efficient through training, controls and automation, instead of creating a new large cost center.

In general, basically all departments within a company are considered to be GRC stakeholders. Board and supporting committees depend on the output of GRC processes in order to be informed and to be able to make fast decisions. They as well set up strategy, policies and objectives. Management teams need to have clearly defined roles and responsibilities. System departments need to ensure required level of safety and alignment of IT projects with business strategy. They need to have recovery plans for emergency cases as well. Internal auditors prepare and realize efficient audit plans and programs and make sure that they are corresponding with strategy and goals of the organization. Legal department is then performing permanent tasks and coordinating compliance efforts throughout the company. [9]

2.1.5 The most common GRC challenges

Companies are nowadays facing many GRC challenges, usually more of them at one time. The following paragraph is identifying the most common challenges that organizations need to deal with regardless their size or industry they are operating in. [21]

- **Complexity of management systems and GRC programs**. Excessive complexity is caused by lack of oversight from executive management, by missing company standards and policies, deficient processes, control gaps and ineffective GRC platform that is not able to provide required transparency. Recent researches proved that corporate leaders represented by boards are still not performing sufficient oversight activities. The report then states as well that a lot of organizations are using for Microsoft Word and Excel for their GRC processes. They are then not transparent, inefficient and a lot effort, even double effort, needs to be dedicated to them. These organizations can't respond to any risk or event fast enough.

- **Inability to manage complexity and reduce GRC costs**. There are usually global GRC programs existing next to the country-specific ones. This set up is causing increased administration costs, activities are duplicated, participants in the related processes need to often perform the same tasks repeatedly. The organization is not able to formulate common standards and compliance programs and multiple assessments are provided to the stakeholders.

- **Alignment of GRC processes within the whole organization**. There is not unified system that goes through the whole company. Different parts of an organization are using different "language", different compliance metrics and standards.

- **Intellectual property and privacy protection**. New technologies are bringing new challenges. The still increasing usage of cloud computing, big data, analytics tools, social networks and mobile devices are representing new potential risks that the

company needs to deal with in order to keep intellectual property and confidential data secured.

- **Cybersecurity risks**. The research proved that investments in cybersecurity are still relatively low. Companies are underestimating this kind of risk although the attacks are still more frequent and more sophisticated.
- **Mobile strategy**. Almost half of the companies allow usage of personal devices at work. It is a current trend to support the integrity of private and work life. By usage of private devices, this line is blurred but the risk of potential data loss is increased. Internal policies often fail to address all the needed rules and regulations. Furthermore, the awareness of employees to potential risks is still low.
- **Supply chain risk**. Supply chain risk is represented by issues related to company's network of suppliers, distributors, vendors and other business partners. The risks are represented by the reliability and integrity of the partners, by transactions and data exchange. Heavily used outsourcing of services is making this challenge crucial to companies today.

2.2 Legal regulations

Sarbanes-Oxley Act (SOX) is an US federal law regulating corporate finance and business environment as such. It came into force in July 2002 and the main goal was to ensure transparency and accuracy of accounting and financial statements, to establish internal control systems and to identify any discrepancies and thus a possible frauds. The main reason, why SOX was formulated, was a number of accounting scandals that were revealed in previous years. SOX requires, that US-listed companies have their own system of internal controls and directors report and monitor risks.

In a similar way, standards are raising elsewhere, and the mixture of the International Financial Reporting Standard (IFRS) outside the United States means that a convergence is occurring in financial reporting and its requirements. The list below describes how SOX is defined around the world. [10]

- **J-SOX, Japan**. The Japanese Financial Instruments and Exchange Law was declared in 2006 and it is followed since 2008. This law is also inspired by corporate scandals and became affectionately known as J-SOX. This law dictates listed companies and their subsidiaries to implement a management assessment of controls on their financials reports. Expectation of J-SOX is to prompt mass audit automation in similar way as in United States.
- **CLERP-9, Australia**. CLERP is a shortcut for Corporate Law Economic Reform Program introduced in 2004 to strengthen Australia's financial reporting framework. The main idea of CLERP is not to be as prescriptive as SOX. It contains reform to the existing corporate governance provisions. It also includes changes to financial reporting an executive reward. To ensure auditor and analyst independence, provisions are in place.
- **C-11, Canada**. C-11 was introduced in Canada, in 2005 and it has established a procedure for the detection of misconduct in the public sector. It also secure protection for the person who discloses these, because protection of informant is also part of SOX.

- **Basel II, Switzerland**. Basel II defines an international standard for banking. It can be used by regulators when making regulations about bank capital to offset potential risk. If the risk is on high level, then capital of bank should be higher to ensure, that bank stays solvent. This claim proactively provides a big safety net for banks and their customers.

- **Combined Code of Corporate Governance, England**. In England, similar to many other countries, legislation has been changed as the response to corporate scandal. For example financial scandal in *Polly Peck* and *Maxwell*. Quiet few reports were created to deal with many governance issues. Best known, Hampel Report, started the Combined Code of Corporate Governance in 1998. Some areas of this document covers the structure and operations of a company board, directors pay, responsibilities of institutional shareholders or accountability and audit.

2.3 Other terms

Segregation of duties is an internal process that should prevent any errors and frauds. The process is designed in the way that ensures that one employee is not the only person who is responsible for certain task from the beginning to the end and is not the only one participant in the respective process. The process is divided into smaller tasks and the control by another person is applied. Apart from this separation of activities, other commonly used principles are, for example, four eyes principle, two signatures principle or several factors contributing to completion. Segregation of duties helps to increase security and prevent potential risks, but it is resulting in higher operational costs. This is one of the reasons, why segregation of duties is applied by the companies only to the most sensitive processes where considerable harm could be caused.

Access control and roles. Management of permissions and control of access to the internal systems are key features for ensuring security and compliance. Companies need to establish authorization concepts and define what respective users can access, view and edit. The main elements of the so called role-based permission concept are permission groups, permission roles and target groups. Permission group defines the group of users who share specific attributes and who will be granted a specific role. The group could be defined by department, for example all HR employees, by location or by any other attribute. Permission role is a set of permissions that specifies the parts of the system, transactions and fields that the user group with this role can access, view or edit. Granularity of the permissions varies for different systems and sometimes even for different modules and sections of one particular system. Target group is then a group of users whose data can the users with the respective permission role access.

Chapter 3

GRC Software Solution

As GRC is a crucial part of management of all bigger companies, the demand for a complex solution is enormous. There are nowadays many vendors who are providing various software dealing with this topic. GRC is a wide area and software providers are mostly focusing on just some parts of it. When choosing the right software, companies therefore need to do firstly a deep analysis of internal environment. Then analysis of available systems needs to be performed, so they are able to select the software solution that deals with their GRC requirements in the most efficient way.

The following chapter is listing the best known complex GRC software solutions that are currently available on the market and that are covering basically all areas of GRC.

3.1 SAP BusinessObjects GRC

SAP BusinessObjects GRC covers three important activities: analysis, management and monitoring. These are main capabilities of every effective GRC software solution and supporting technologies.

There are four native parts of the SAP solution. It is Access Control, Process Control, Risk Management and Global Trade Services. These systems are combined into unified work space, so the user interface is the same and the users can use all the systems without any need of additional trainings. Sharing of selected data and functions is enabled among the systems as well. SAP BusinessObjects GRC is integrated with many other systems and applications.

Figure 3.1 shows an example of reporting with SAP BusinessObejcts GRC. This particular report is created using SAP Treasury and Risk Management solution.

3.1.1 SAP Access Control

SAP Access control is an application that specifically looks at what access people have in an organization. With starters, movers and leavers, appropriate access can be a real concern. Employing proper Segregation of Duties (SoD), governing enterprise roles, provisioning users, and granting audited emergency access for super users is key to managing organizational risk. SAP Access Control consists of Access Risk Analysis, Business Role Management, Access Request Management, Emergency Access Maintenance and some other add-ons. The structure is displayed in Figure 3.2. [19]

Figure 3.1: Reporting with SAP BusinessObejcts GRC. Source: [16]

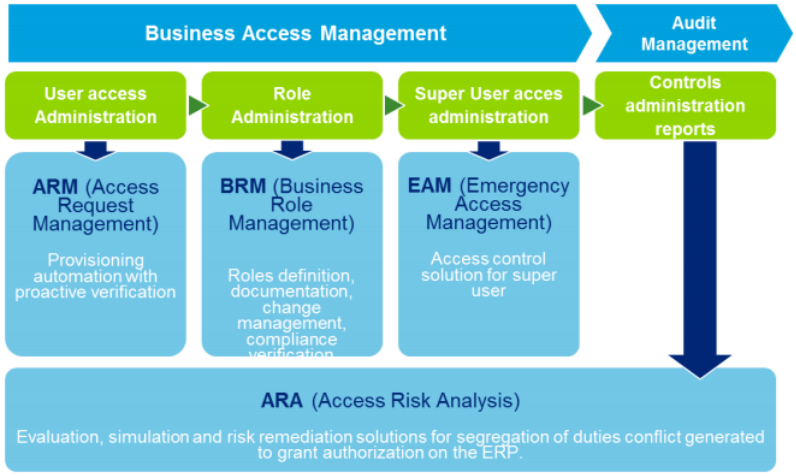


Figure 3.2: The structure of SAP Access Control. Source: [9]

Access Risk Analysis is a tool that represents security audits and analyzes any possible violations of SoD. It identifies SoD, then analyzes it and in the end solves all the issues coming from the performed audit.

Business Role Management defines roles and manages the procedure handling roles. In enables role definitions, development, testing and maintenance.

Access Request Management enables the automation of the process dealing with access requests. It reduces significantly workload for IT staff and prevent potential risks related to errors in the approval process and violation of SoD by integration with Access Risk Analysis.

Emergency Access Maintenance monitors activities done by so called Superuser or Firefighter, who has a wide access rights. This Superuser should, however, be used only in case of extraordinary situations, as it enables regular users to perform tasks they are not entitled to do from the definition of their standard role.

3.1.2 SAP Process Control

SAP Process Control is a widely customizable software solution for process control management. It protects the company against fraud, waste, rules violations and errors. The protection is performed via deep analysis of company's processes and activities. It gives the company insight into the compliance status of the controls in place across key business processes, aligning them with risk prevention. SAP Process Control is a combination of various data forms, workflows, certifications and reports. It offers among others following key functionalities: [19]

- support of both internal as well as external audits;
- documentation of control environments;
- testing and assessment of controls;
- reducing of auditing costs due to acceleration of audit processes and cycles;
- review of process control and risks;
- support of corporate compliance programs;
- improvement of performance with help of identification and focus on crucial risk areas.

3.1.3 Risk Management

SAP Risk Management is a solution that documents, monitors, and reviews risks. It helps companies to reduce risk by systematically identifying and managing risks in order to prevent any incident in the future. It supports all the crucial processes: identification, measurement, monitoring, responding. [9]

With SAP Risk Management risks can be analyzed in different ways. It is done through analysis of various **Key Risk Indicators (KRIs)**. KRI is a measure that estimates, how likely the risk is to occur. KRIs can be either quantitative or qualitative. During system implementation SAP consultants guide the customer how to set up useful and effective KRIs. They should be understandable, accessible across all business areas and locations, defined in a cooperation with the whole company. If they are implemented properly, they

are able to highlight trends and raise warnings. KRIs can use data from various (even non-SAP) systems like SAP ERP Financials, SAP Supply Chain Management, SAP Human Capital Management and many others. [19]

3.1.4 Global Trade Services

SAP Global Trade Services (SAP GTS) manages the risk globally. It helps companies to accomplish more efficient management of international trade operations, automate trade compliance and handle the supply chain across the borders.

SAP GTS consists of SAP Compliance Management, SAP Customs Management, SAP Risk Management and SAP Electronic Compliance Reporting. **SAP Compliance Management** performs all activities related to control of imports and exports. It deals with licensing requirements, legal regulations, embargo checks end other topics. **SAP Custom Management** handles processes related to custom and transit procedures and goods classification. **SAP Risk Management** within SAP GTS is focusing on risks related to vendors, documents and goods. **SAP Electronic Compliance Reporting** then enables regular issues of declarations. [20]

3.1.5 Benefits of SAP GRC

Increased transparency is one of the key benefits of SAP GRC. It enables and automates the enterprise identification, monitoring and mitigation of risks through lines of business. It provides transparency and visibility of risks through the enterprise to allow organizations to be more responsible and make more effective business decisions while considering all potential risks.

Availability of all kinds of data that can be then processed further, is one the main benefits of GRC software solution provided by SAP. With SAP solution all the information can be leveraged wherever and whenever it is needed. It extracts data from massive data stores of systems in SAP landscape. It can also access information stored in non-SAP enterprise applications. For example e-mail system, spreadsheets and other documents.

Alignment and consolidation of risk management with corporate strategy is as well a required feature that is delivered with SAP GRC. Effective strategic management involves a consolidated view of goals, underlying key performance indicators (KPIs), strategy execution initiatives and related risks.

For most of the companies the benefit of better **decision-making** based on more information is very important. With this solution all essential information can be quickly provided and more knowledgeable decisions based on all important risk factors can be quickly done. It allows the decision-makers to manage various what-if cases as well. [18]

3.2 Oracle Enterprise GRC manager

Oracle responded to the need of risk management with a product called Oracle Enterprise GRC Manager. With this product, customers can standardize the process of identifying, measuring and responding to operational risk. Furthermore they can highlight key risks and performance indicators via executive-level dashboards that can be drilled down to detailed evidence in source systems.

Oracle's solution helps the companies to automate segregation of duties enforcement through enterprise applications, database systems and custom solutions. The central es-

tablishment of user access combined with authorization policies ensure the prevention of possible fraud. Systems are automatically analyzed to ensure that critical layouts follow standard policy and change management processes.

Compliance activities are developed against documented policies and the best known control frameworks such as COSO or COBIT. Protection of critical information assets is used at all levels. Core privacy and security controls with automated enforcement of correct user access and authorization policies keep information safe through all IT resources such as database, applications or middleware.

Oracle GRC is composed of three main components: GRC Intelligence, GRC Manager and GRC Controls is displayed in Figure 3.3.

GRC Intelligence provides insight into the compliance readiness and ability to respond to any event. It plans, defines and reports GRC activities in the whole organizations. It has a wide scale of analytics tools and dashboards.

GRC Manager is a central storage of all related documentation referring to all GRC components like crucial company policies, processes, controls, risks and issues. It is performing the tests and controls and initiating related processes. After the testing is completed, it is archiving the results.

GRC Controls consists of four solutions. Application Access Control Governor performs the controls of SoD. Transaction Controls Governor monitors policies and processes performed in Oracle ERP system. Preventive Controls Governor should ensure the prevention of any violations and issues. Configure Controls Governor then integrates data and applications and audit key changes done in configuration.

Figure 3.4 shows an example of screen of GRC solution from Oracle.

3.3 IBM OpenPages GRC Platform

Using IBM OpenPages customers can manage risks and initiatives in all areas of GRC across the company. That helps companies to reduce losses, improve decision making regarding allocation of resources and optimize business results. It enables companies to integrate risk management processes across the enterprise, manage risk and compliance in accordance with various requirements, such as Basel II or SOX, regulations on the creation of financial reports, data privacy and other regulations.

Figure 3.5 shows an example of screen of GRC solution from IBM.

With IBM solution the companies can also effectively use GRC information in order to make better business decisions. It provides many tools for creation of customized reports and identification of current trends. OpenPages is a set of following tools:

- OpenPages Operational Risk Management - Identification, management, monitoring and analysis of operational risks across the enterprise through a single integrated solution.
- OpenPages Policy and Compliance Management - Consolidation of processes, policy management and compliance in a single solution and management changes in regulations and interaction with regulators.
- OpenPages Financial Control Management - Automation of management processes of financial engineering instruments in accordance with the reporting requirements arising from the SOX and similar global regulation.

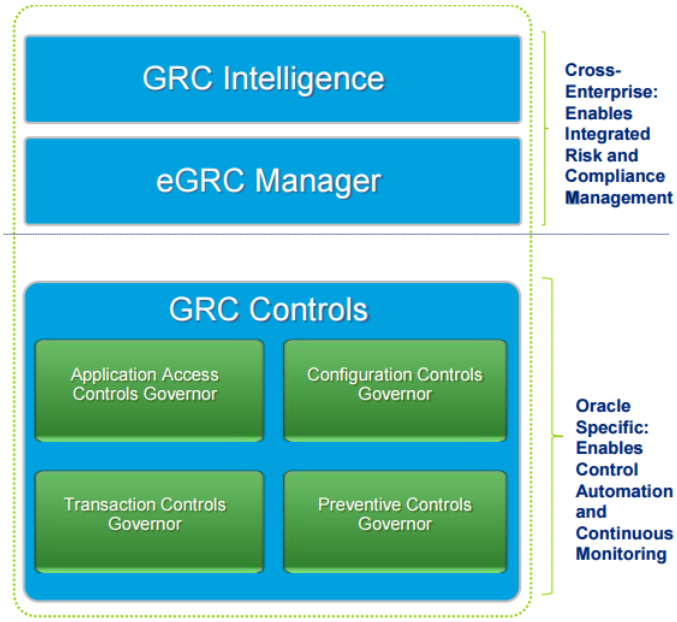


Figure 3.3: Structure of Oracle GRC. Source: [9]

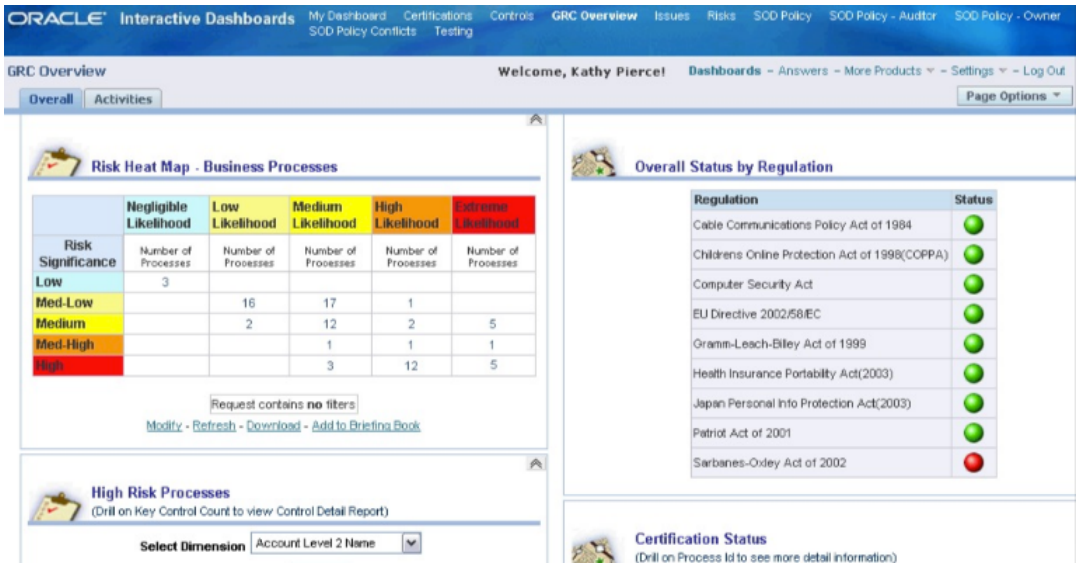


Figure 3.4: Example of GRC Overview from Oracle. Source: [2]

- OpenPages IT Governance - Sustainable approach to IT risk management and compliance that enables to respond to the issue of sensitive data, management of technology assets and ongoing changes in regulatory requirements.
- OpenPages Internal Audit Management – Automation and management of internal audits across multiple organizations and effective implementation of broader risk management activities and compliance.
- OpenPages GRC Platform - Wide knowledge base of the activities of risk management and compliance across the enterprise.

3.4 RSA Archer eGRC

RSA Archer eGRC **unifies** corporate governance, risk and compliance management on a single platform. It helps significantly manage system complexity and reduces training time for the users. It is claimed to be the most configurable and **flexible** software compared to the previously mentioned solutions. It enables companies to constantly add new tools, create new reports and modify the processes on the fly. As the platform is flexible, it can be implemented in a small scale and then extended later if needed. It is easy to use for users, who then do not need to have technical skills. The user interface is highly configurable as well. The platform supports integration and **collaboration**, so the users across the whole system are using the same processes and data. [9] Figure 3.6 shows an example of RSA Archer screen.

RSA Archer eGRC solution consist of more components. **RSA Archer GRC Platform** is a common foundation for all the programs. It integrates the programs and data are shared effectively. **IT and Security Risk Management** component establishes security policies and standards. It is able to identify attacks and respond to them. **Regulatory and Corporate Compliance Management** makes sure that the company is compliant with all relevant legal regulations. It forms a complex framework of controls. **Enterprise and Operational Risk Management** understands the business context and the operational risk the respective company can face. **Business Resiliency** monitors, if the company is prepared for any unexpected event that could come and cause a loss. Critical values and core assets need to be identified and then protected. Business Resiliency helps companies get ready for any disruptions, resolve quickly any incidents and manage crisis. **Audit Management** is crucial part of RSA Archer. It provides independent testing of corporate compliance and other objectives related to GRC. [4]

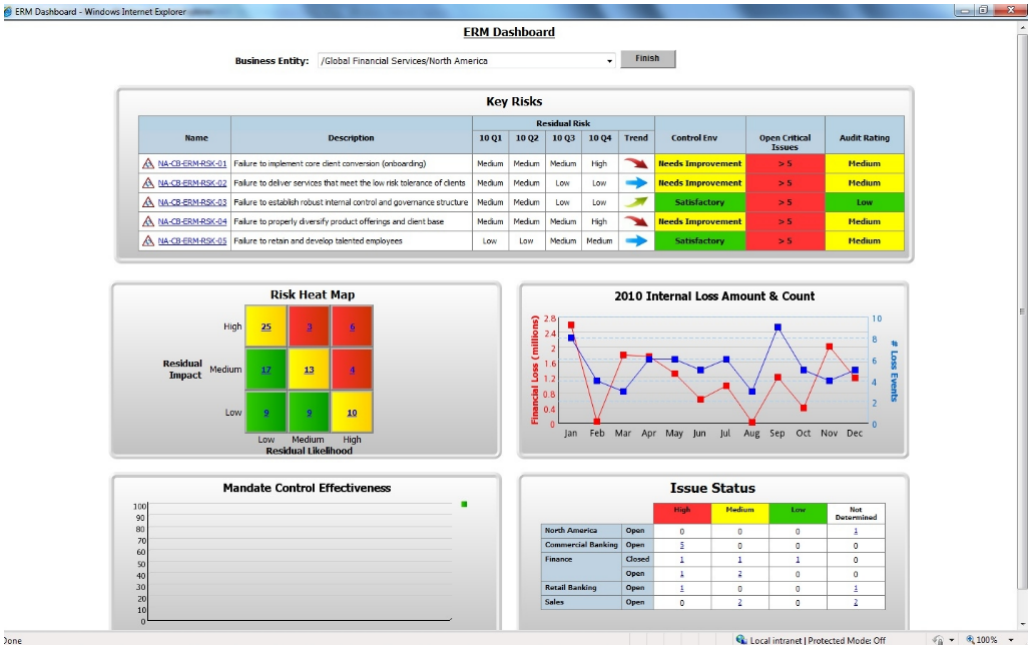


Figure 3.5: Example of GRC solution from IBM. Source: [3]

Figure 3.6: Example of RSA Archer screen. Source: [1]

Chapter 4

SAP back-end Technologies

This chapter provides a brief overview of SAP HANA Platform. SAP HANA Platform is a technological innovation introduced by SAP to enable fast processing of analytical data and exploit the potential of rapid development of hardware and reduction of its costs. The first section gives a short description of SAP HANA technology and some of its advanced features. Detailed description of SAP HANA Platform can be found in my bachelor thesis [23], or in a book A Course in In-Memory Data Management from Springer written by Hasso Plattner. [17]. The second section is an introduction to the Core Data Services. This feature is based on SAP HANA and it is an enhancement of SQL for defining semantically rich database tables or views and user-defined types in a database. At the end of this chapter, cloud technology provided by SAP is described in detail.

4.1 SAP HANA platform

SAP HANA is revolutionary application and database platform developed by SAP, which enables fast processing of large volumes of data in real time as well as their immediate analysis. With SAP HANA it is possible to achieve very fast response to the queries. Comparing to the regular SQL database, the processing time is much shorter.

One of the key features of SAP HANA is the location of entire databases in RAM. When referring to this concept it is spoken about „in-memory“ processing. It means that the data is not stored primarily on the hard drives. The data access and all the following operations are therefore executed faster. The hard drives are still in use but just to store passive data or for recovery purposes. The standard process to enable recovery is regular creation of logs. Data is written into log files and those files are stored in a persistent memory. This is an important process that can guarantee the durability in enterprise applications based on Atomicity, Consistency, Isolation, Durability concept(ACID). These properties guarantee reliability for database transactions and are considered as the foundation for reliable enterprise computing.

Another crucial feature of SAP HANA is a way of storing information. Unlike conventional SQL database, data is primarily stored in columns, rather than in rows. In practice it means that if the database contains, for example, data on residents of the Czech Republic, there are certain surnames that keep occurring a lot (e.g. Novak), but as data are stored in columns, the respective surname is stored in the column only once and will be therefore looked up faster. However, line storage is supported in SAP HANA as well

SAP HANA is not only a database, it is also a powerful application server with many features already prepared with the support of HTML5. Among other things, it significantly accelerates the development of new applications and allows them to achieve high performance on mobile devices such as smartphones or tablets.

4.2 SAP HANA Cloud Platform

SAP HANA Cloud Platform (HCP) is an in-memory cloud platform based on open standards for rapid development of on-demand applications. The platform contains a comprehensive set of services for integration, collaboration, enterprise mobility and analytics. It enables customers to rapidly build, manage and deploy cloud-based applications that complement and extend non-SAP or SAP solutions. It is based on Platform as a Service (PaaS) concept. From technical perspective, this platform is not so different from application systems that are installed on-premise. The main difference is that SAP takes responsibility for purchasing and maintaining the whole infrastructure, such as hardware, software and other related concerns. It is possible to use the following programming models to build applications in HCP: [26]

- **Java** – HCP is Java EE 6 Web Profile certified. It is possible to develop Java applications in similar way as for any application server.
- **SAP HANA** – development tools to create comprehensive analytical models in SAP HANA are included in HCP. It is possible to build an application with SAP HANA programmatic interfaces and integrated development environment.
- **HTML5** – lightweight HTML5 applications in a cloud environment can be developed in HCP.
- **SAPUI5** – in HCP it is possible to use the UI Development Toolkit for HTML5 for developing user interfaces for modern Web business applications.

SAP HANA Cloud Connector (SCC) serves as a link between existing on-premise systems and on-demand applications in HCP. It combines easy configuration with a clear setup of the systems that are exposed to HCP. It allows users to control the resources available for the cloud applications in those systems. It runs as on-premise agent in a secured network and behaves as a reverse invoke proxy between the on-premise network and HCP. It is not necessary to configure the on-premise firewall to allow external access from the cloud to internal systems, when SCC is in use.

It is possible to use SCC in business critical enterprise scenarios. It ensures that any broken connections are automatically re-established. It can be run in a high-availability setup and it provides audit log of the inbound traffic, or configuration changes. When users do not want to use SCC, it is possible to open ports in firewall and use reverse proxies to establish access to on-premise systems, but SCC has following advantages: [26]

- An inbound port to establish connectivity from SCC to an on-premise system does not have to be opened in firewall of the on-premise network.
- By using SCC we can use additional protocols, apart from HTTP. It is possible to use the RFC protocol, which supports native access to ABAP systems by invoking function modules.

- The propagation of cloud users identity to on-premise systems in a secure way is allowed by SCC.
- SCC can be used in the opposite way. When users need to connect on-premise system to the cloud.

In Figure 4.1 SCC configuration overview can be seen.

4.3 Core Data Services

Core Data Services (CDS) is an infrastructure that database developers can use to create the persistent data model, which passes the application services to UI clients. Developer can define the analytical and data persistence models that are used to transfer data in response to the client HTTP request. CDS allows to define a persistence model that contains objects such as views, tables and structured types. These objects specify data and the way of its consumption by applications.

The first step in the process of developing applications providing the access to the SAP HANA database is building a data model in the back-end. After the underlying data model is created, the front-end developer can create application services that consume elements of the data model. Client applications then bind buttons, graphs, charts or other UI controls to the application services to display the requested data to the user.

In SAP HANA Extended Application Services (SAP HANA XS) data model is mapped to the consumption model that is passed to users and client applications. Data can be displayed and analyzed in the corresponding form in the client application interface. SAP HANA XS enables developers to create views, tables and sequences in the repository. These repository object can be used by any front-end applications. When implementing data model, developer can choose from CDS syntax or HDBtable syntax. HDB table syntax includes the different configuration schema for all of the various design time data artifacts such as `.hdbsequence, .hdbtable, or .hdbview`. All repository files can be transported to other SAP HANA systems through a delivery unit. A delivery unit is the part of SAP HANA that enables you to assemble all your application related repository artifacts altogether into an archive that is easy to import to other systems.

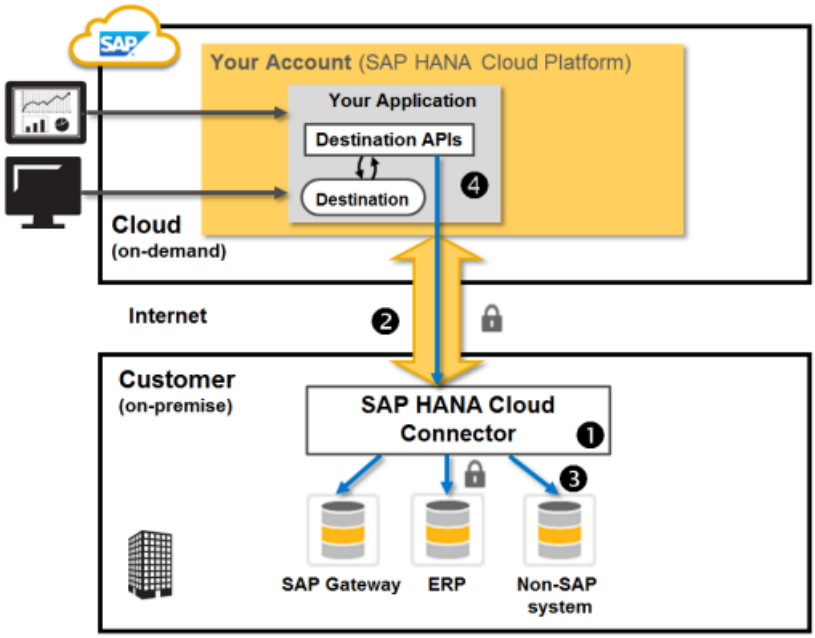


Figure 4.1: SAP HANA Cloud Connector configuration. Source: [6]

Chapter 5

SAP front-end Technologies

This chapter is focused on evolution of user interface in SAP software. The best known SAP dynpros are being replaced by new technologies such as Web Dynpro or Fiori applications, because they are much more user-friendly and easier to access. In recent years SAP needed to react to customer needs. Therefore complex and confusing screens have been simplified and divided into well-structured applications for single use. Table contents have been supplemented with graphs and graphic design standard has been redesigned for web browsers using HTML5 and Javascript.

It is really important for modern software companies to focus on mobile devices. Smartphones and tablets make it easy to access applications, services and content in business or private life. One of the goals of SAP strategy is therefore to deliver attractive and easy to use applications that enable the users to achieve as quickly as possible what they intended to do.

5.1 ABAP Dynpro

ABAP Dynpro is a shortcut for dynamic program in ABAP. It is a historic framework that was introduced in 1992 with launch of SAP R/3. This dynamic program can be used to create screens with a large set of UI controls. To process logic of this type of screens ABAP programmer is using so called process before output coding (PBO) and process after input coding (PAI). PBO is a type of event that is triggered when screen is rendered and the developer can define default values or buttons labels and texts. PAI is then an event that is triggered when the user submits or leaves the screen. It includes input checks, submit actions or navigation between screens. A huge number of existing applications is written in ABAP Dynpro and customers complain about its complexity and unattractive look. Example of ABAP Dynpro application used to create business partner can be seen in Figure 5.1.

5.2 ABAP Web Dynpro

Web Dynpro for ABAP is a standard UI technology used by SAP developers for creating Web applications in the ABAP environment. It is a mixture of graphical and runtime development environment with special Web Dynpro tools that are included in the ABAP workbench. [27]

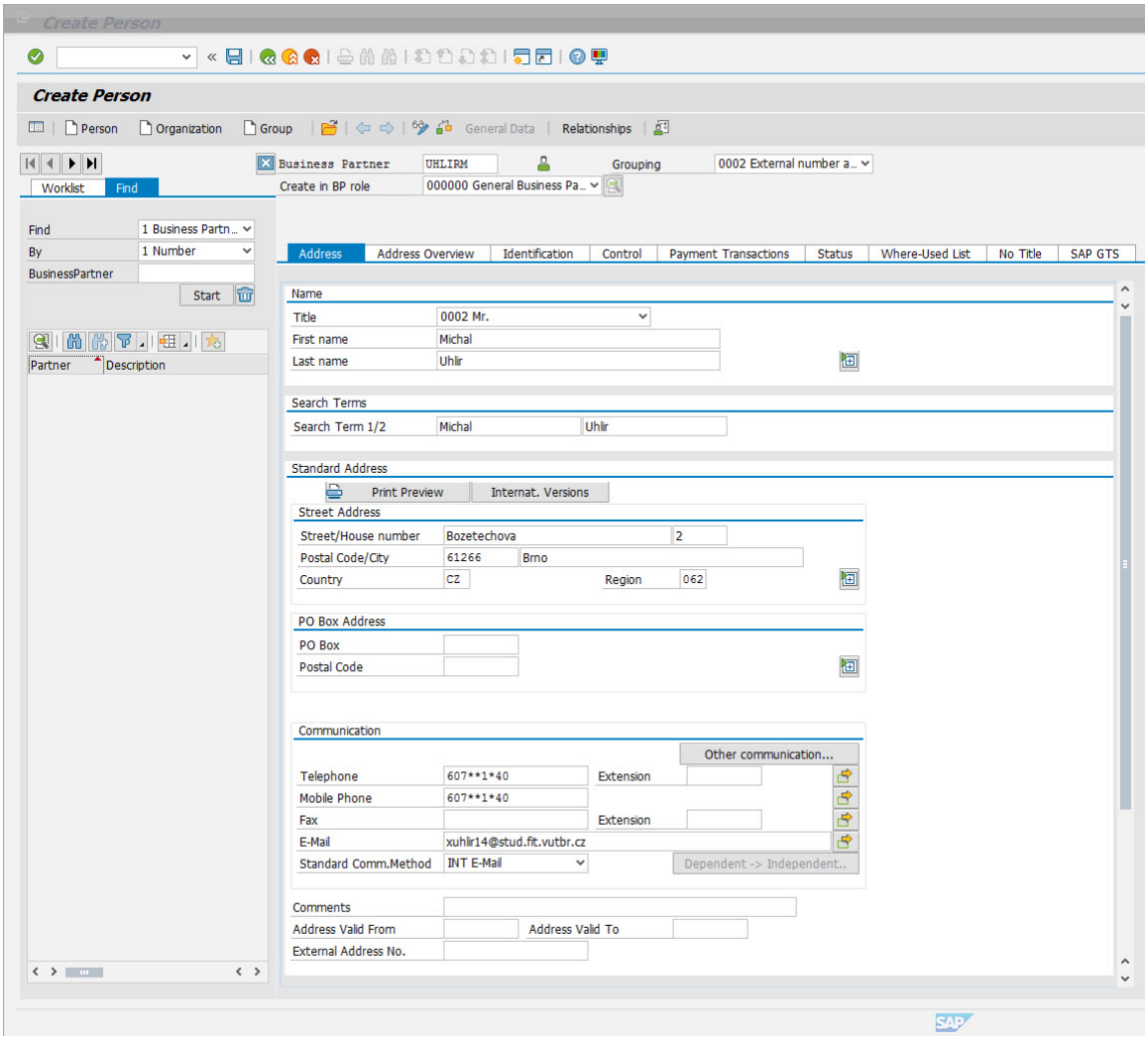


Figure 5.1: ABAP Dynpro screen to maintain business partner.

This feature enables developers to strictly separate layout from business data. The navigation and layout can be easily changed using the Web Dynpro tools. If data types and domains are defined properly, automatic input checks are executed automatically. It is a native feature of Web Dynpro. All Web Dynpro applications are structured according to the Model-view-controller (MVC), which is a widely used programming pattern. The model forms the interface to the back-end system and accesses data. The view is just presenting the data on the front-end. The controller then processes the entries made by the end users and passes them to the model. Simple example of Web Dynpro is introduce in Figure 5.2.

All objects created during Web Dynpro development are fully integrated in ABAP lifecycle management. They can be then transported and translated in ABAP workbench, which is a set of tools used by ABAP developers. Customers can then make their own enhancements.

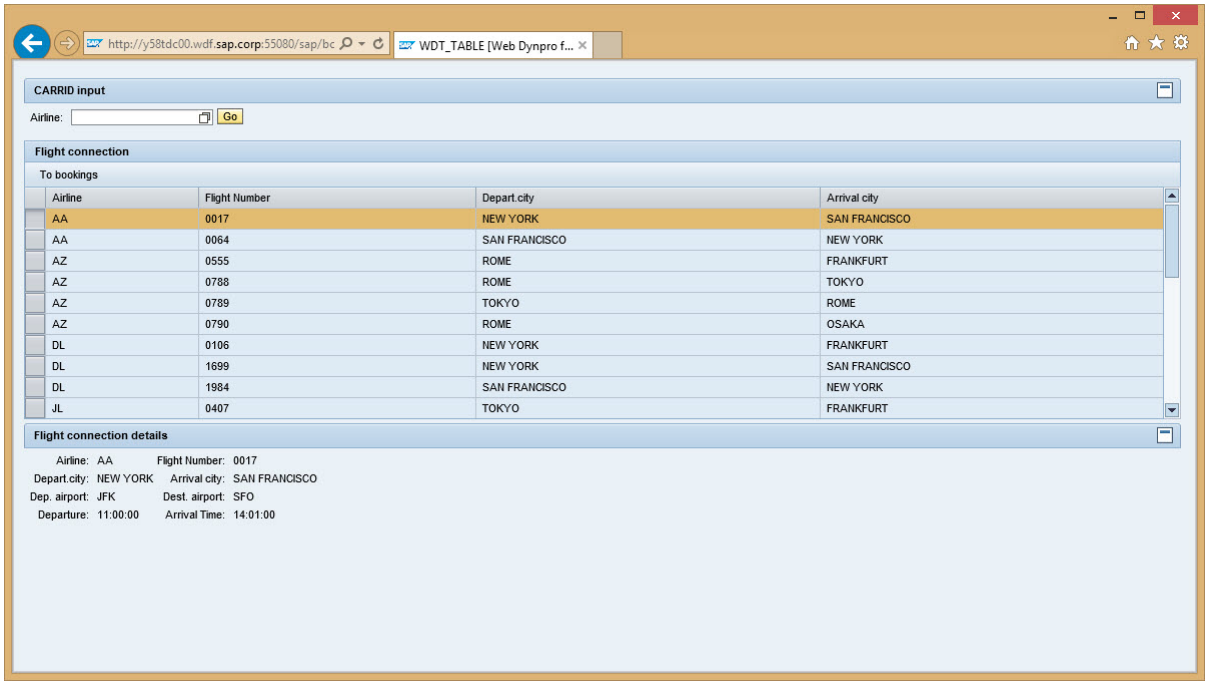


Figure 5.2: Simple Web Dynpro based example application.

5.3 Floor Plan Manager

SAP Floor Plan Manager (FPM) is a framework based entirely on ABAP Web Dynpro. It is used for model-based and declarative creation and adaption of user interfaces. With the help of predefined UI elements such as toolbars, floor plans or generic user interface building blocks, it ensures consistency across applications and compliance with SAP UI design guidelines.

By using FPM, you can greatly reduce the time required to create such applications. Central functions, such as messaging, navigation and personalization, are all embedded functionalities in this framework and application programming interfaces easily defining them. FPM Configuration Editor, known also as Flexible User Interface Designer (FLUID), is a powerful tool that allows the user to configure the application composition as a whole, or as the individual floorplan and generic UI building block inside. The design of FPM follows the SAP user interface design guidelines and policies. Simple applications can be adjusted by configuring the underlying Web Dynpro components, so no additional programming is needed.

FPM is also fully integrated into standard SAP lifecycle management with corrections, transporting, versioning, or translation capabilities. It enables a developer to generate applications based on the business objects and their relations. To create the layout of the individual UI building blocks and make a decision which content to show or hide What You See Is What You Get editor (WYSIWYG) can be used. It is included in FPM. Example of FPM application is shown in Figure 5.3.

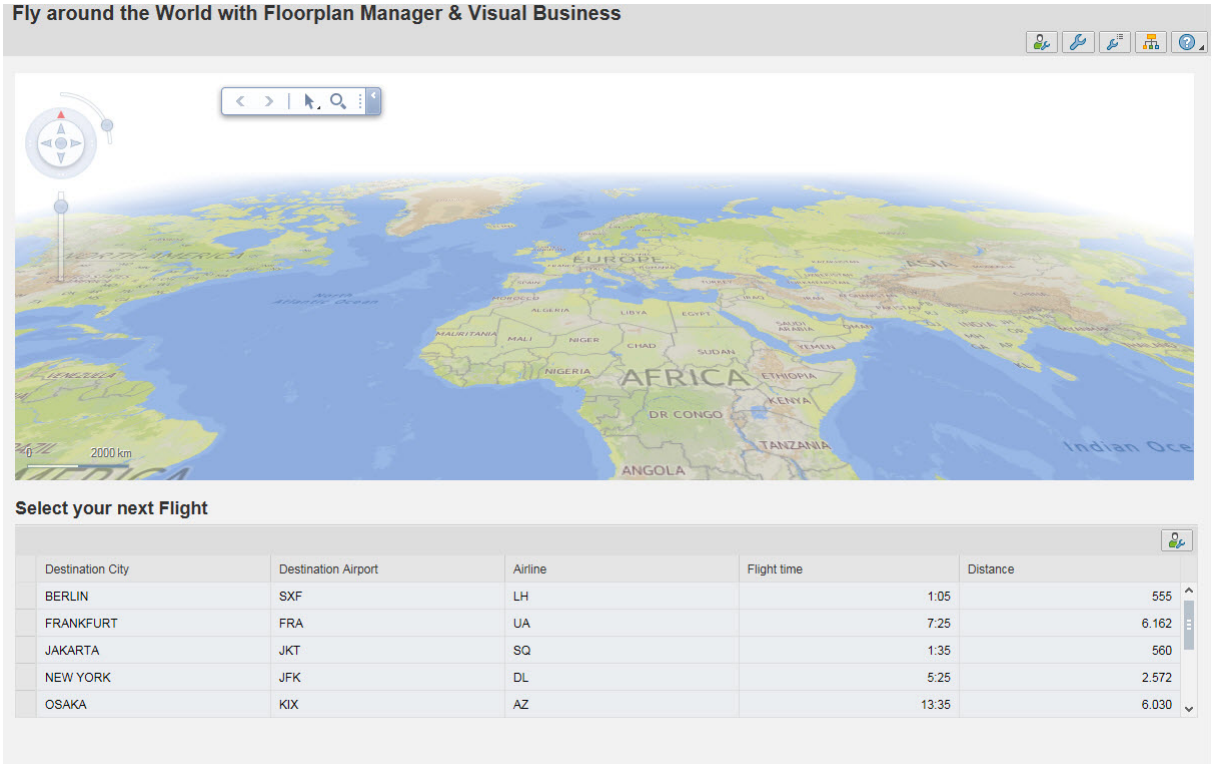


Figure 5.3: Example of Floor Plan Manager application.

5.4 SAP Screen Personas

SAP Screen Personas allows companies to personalize their system screens for different user roles without any custom development. They can manage different user and group profiles to enhance user satisfaction, optimize productivity and minimize training time on SAP. It is easy to install and very intuitive to use. All the functionalities of the standard SAP GUI are included. Screen Personas allows you to create scripts to automate the process within a transactions. A flavor identifies personalization of a particular transaction and can be assigned to the user role. Each transaction can have more flavors with every screen looking differently. You can also create your own themes for standard transactions to define specific formatting that will be used across several transactions.

The Administrator tool enables the user to administrate all the Personas objects: flavors, icons, themes and images. It offers features such as finding objects marked for deletion or unused objects. Administration can be done from standard SAP GUI or ABAP Web Dynpro application. Screen Personas can be used only for Dynpro screens. Currently there is no way, how to integrate Web Dynpro Apllications, CRM, SRM or mobile applications into Screen Personas. Users can simply access created applications directly from the Fiori Launchpad. Mobile rendering and responsive design are planned for future development of Screen Personas.

5.5 SAP UI Theme Designer

The UI Theme Designer is a browser based tool which allows customers to create their own themes to adapt the appearance of applications. It is one single tool for branding and theming SAP's key user interfaces. The users can use this tool to easily build their own corporate identity themes by modifying one of the theme templates delivered by SAP. It is possible to add a company logo, or change the color scheme. During the work with UI Theme Designer, all changes are immediately displayed in the visualization of the selected preview page. This tool can be used to personalize ABAP Web Dynpro, SAPUI5, FPM or SAP NetWeaver Business Client applications. In Figure 5.4 you can see a changed logo on standard index page of NetWeaver Business Client.

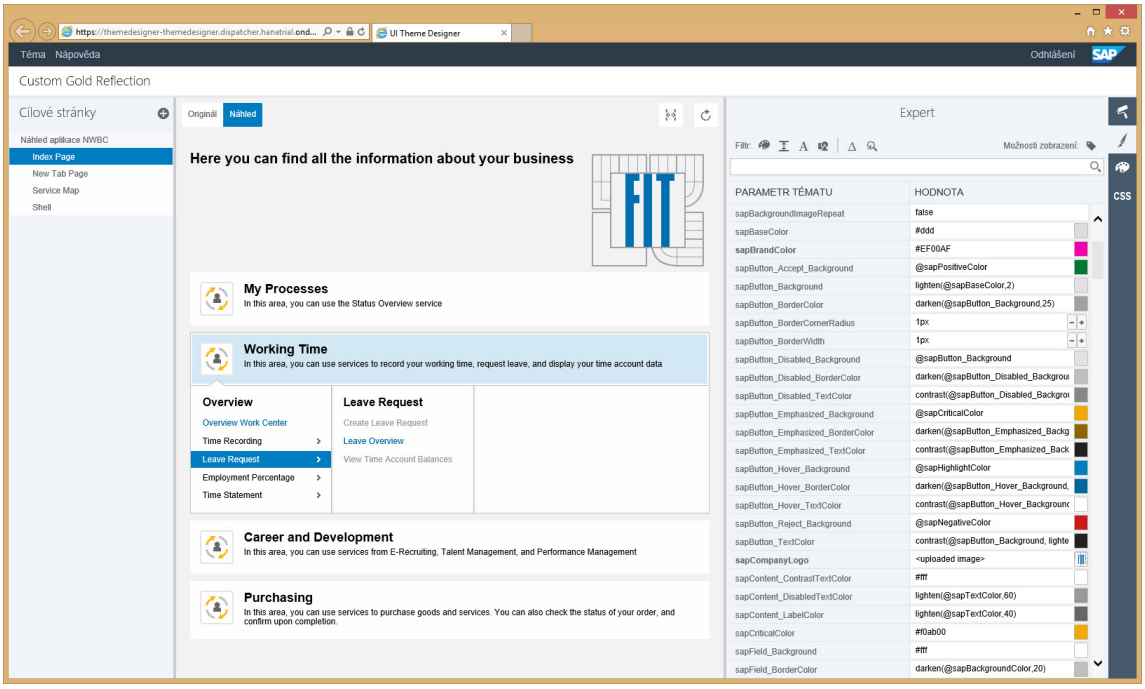


Figure 5.4: FIT BUT logo on standard index page added with SAP UI Theme Designer.

5.6 SAP Fiori

SAP Fiori is a new user experience that brings modern user centric design principles. It provides a role specific and consistent experience through all tasks, for all lines of business. It is very simple to use, personalizable and it runs on any device in responsive way. Organized by user roles, SAP Fiori Launchpad is the root entry element to all Fiori Applications, where users access applications via tiles. Tile is a basic navigation element in Fiori Lauchpad, which is flexible and can be adapted to customer needs. [11]

All user interfaces are built using state-of-the-art technology such as HTML5, SAPUI5 mobile, or Analysis Path Framework (APF). It allows you to access the most recent version of your data through OData services. Using previously created authorizations and roles, you can manage which applications and which data a user can access. In subsections below, basic SAP Fiori technologies and frameworks are analyzed.

5.6.1 SAPUI5

SAPUI5 is a JavaScript based UI library designed to build cross platform business applications using HTML5. It combines all new qualities like flexibility, openness and high speed of innovation with known SAP features like product standard support and enterprise readiness. This toolkit brings many features, rich UI controls for handling predefined layouts for typical use cases and complex UI patterns. Applications are responsive across browsers and mobile devices. Provided UI controls automatically adjust themselves to the capabilities of each device.

Figure 5.5 represents development concepts used in applications built with SAPUI5 library. For example MVC, data binding types, or built in extensibility concepts at code and application level. SAPUI5 enables the users to fully translate their applications to any language. Accessibility features and keyboard interactions are also available. The developers can use HTML5, CSS and JavaScript languages to develop applications that are then run within a browser. Anybody can use an open source version of the UI development toolkit for HTML5 called OpenUI5.

Servers then store SAPUI5 libraries and deploy the applications. You can use an instance on an SAP NetWeaver Application Server or an SAP HANA Cloud Platform to store your applications and libraries, depending on the environment in which you are using SAPUI5. The usual way how the applications access business data is by using the OData model through an SAP Gateway. When the end users open an SAPUI5 application from their device, an HTTP request is raised on the respective server to load the application into the browser. MVC view accesses the relevant libraries and the model is instantiated to fetch the data from the database.

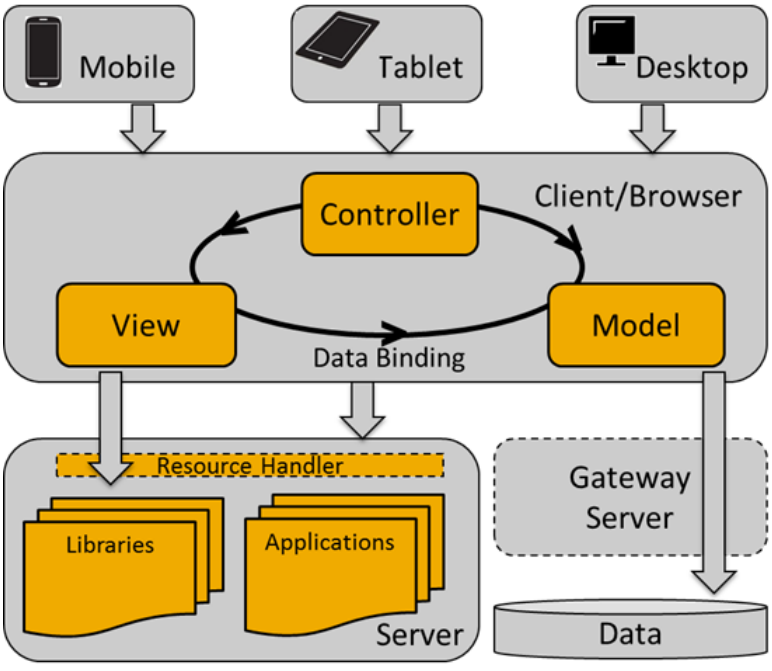


Figure 5.5: Architecture of SAPUI5 applications. Source: [8]

5.6.2 SAP WebIDE

SAP WebIDE is extensible development environment with a huge set of embedded tools including the end to end development process. Developers can use this tool instead of Eclipse based SAP HANA Studio to rapidly design, build, test and deploy their own applications based on SAPUI5. Developer productivity is improved through templates, wizards and interactive code editors. This tool allows developers to collaborate with designers and business experts to fulfill end users expectations and requirements more effectively. Screenshot of SAP WebIDE environment can be seen in Figure 5.6.

Using WebIDE it is possible to create random **mock data** to test your application without connection to back-end system. User can edit this data to have meaningful data to test extension project. It enables to create testing data based on structure of application model loaded from back-end system.

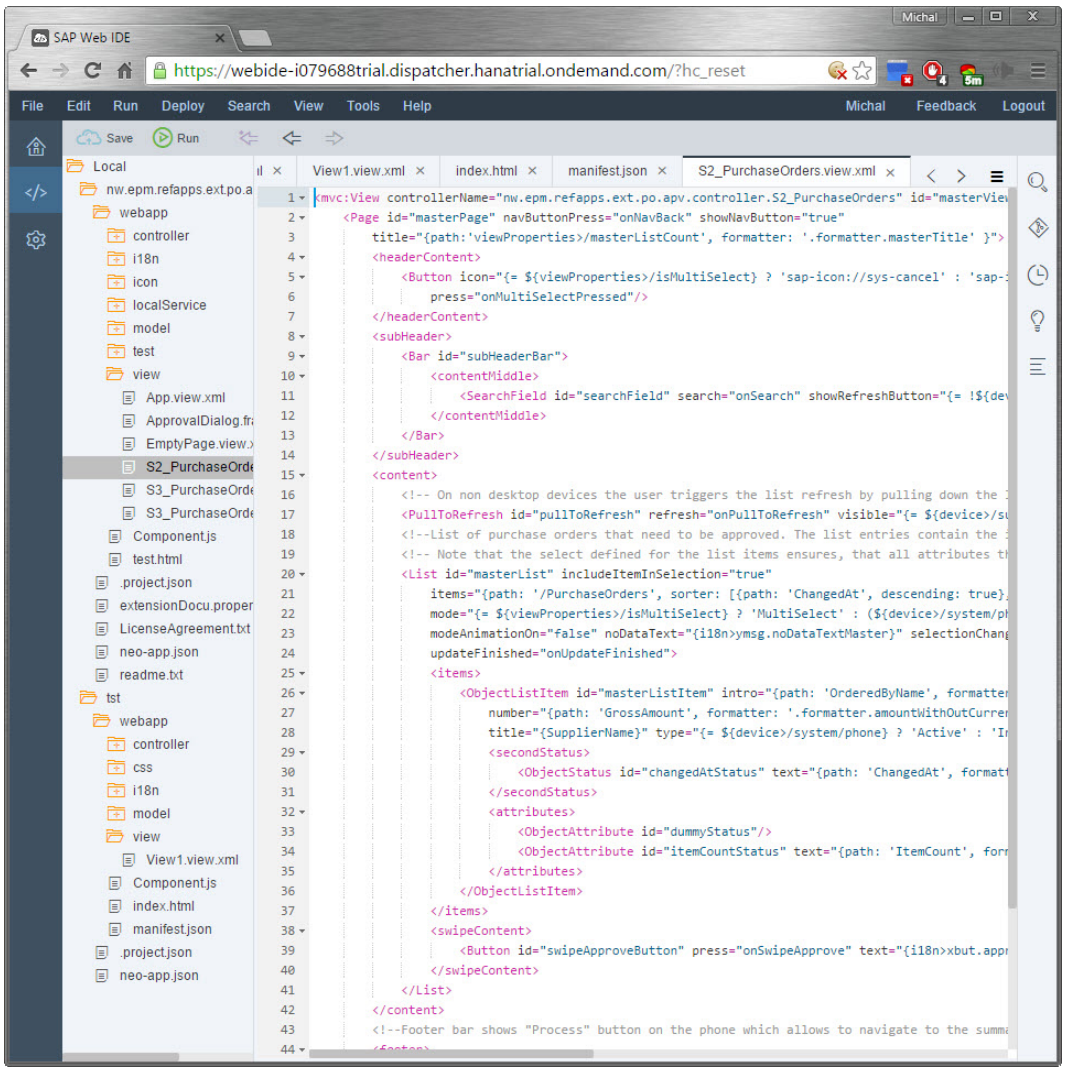


Figure 5.6: SAP WebIDE visage.

5.6.3 SAP Fiori Launchpach

SAP Fiori Launchpad is a basic point of navigation through SAP Fiori applications. It represents a home page of all applications that the users can access on the basis of their role. It provides the applications with services such as personalization, navigation, application configuration and embedded support. The Launchpad displays an entry point with tiles, which can display status indicators, for example number of open tasks with color based on its importance. Each tile is a link to a business application that user can launch, including SAP Smart Business analytical applications and SAP Business Suite transactional applications. For better understanding of concept of SAP Fiori Launchpad and its tiles, see Figure 5.7. The list below provides an overview of SAP Fiori Launchpad concept:

- **Responsive Design** - The visual design of the Launchpad adapts automatically to the screen size of device and shows only the tiles of applications that are supported on current machine. Frequently used applications visually stand out in comparison to the less used applications.
- **Layout Personalization** - Home page tiles are arranged in groups and the user can personalize the layout of this page by moving and removing tiles. Groups can be added, deleted, renamed or reordered. Available tiles can be found in tile catalog, which displays all tiles that the particular user can use.
- **Theming and Branding** - Customer developers can use the UI Theme Designer tool to adapt applications to their brand. More details about SAP UI Theme Designer can be found in section 5.5.
- **Search Capabilities** - Launchpad provides complex search capabilities, including support for SAP Enterprise Search and enable search in the tile catalog.
- **Extensibility** – APIs are provided, so the existing solution can be extended if required.
- **SAP Fiori Launchpad Designer** - The administrators use this browser based administration tool to configure tiles, create home page groups and maintain tile catalogs.

5.6.4 Analysis Path Framework

Analysis Path Framework (APF) is SAP HANA based tool for analytics that provides advanced and complex drill down capabilities. It enables end users to analyze data iteratively by creating analysis paths composed from a sequence of analysis steps. Users can also adapt selections within defined steps of paths that take effect on all following analysis steps.

The purpose of APF is to do the analysis across multiple data sources, to view every step of this analysis at a glance and to modify and store analysis paths for further processing of data. The data is extracted from a database, which provides the ability to handle big data with outstanding performance. Data can be also fetched from different sources. Maintenance of the analysis is done from Analysis Path Configuration Modeler. Screenshot of an example of an application created in the Configuration Modeler can be seen in Figure 5.8.

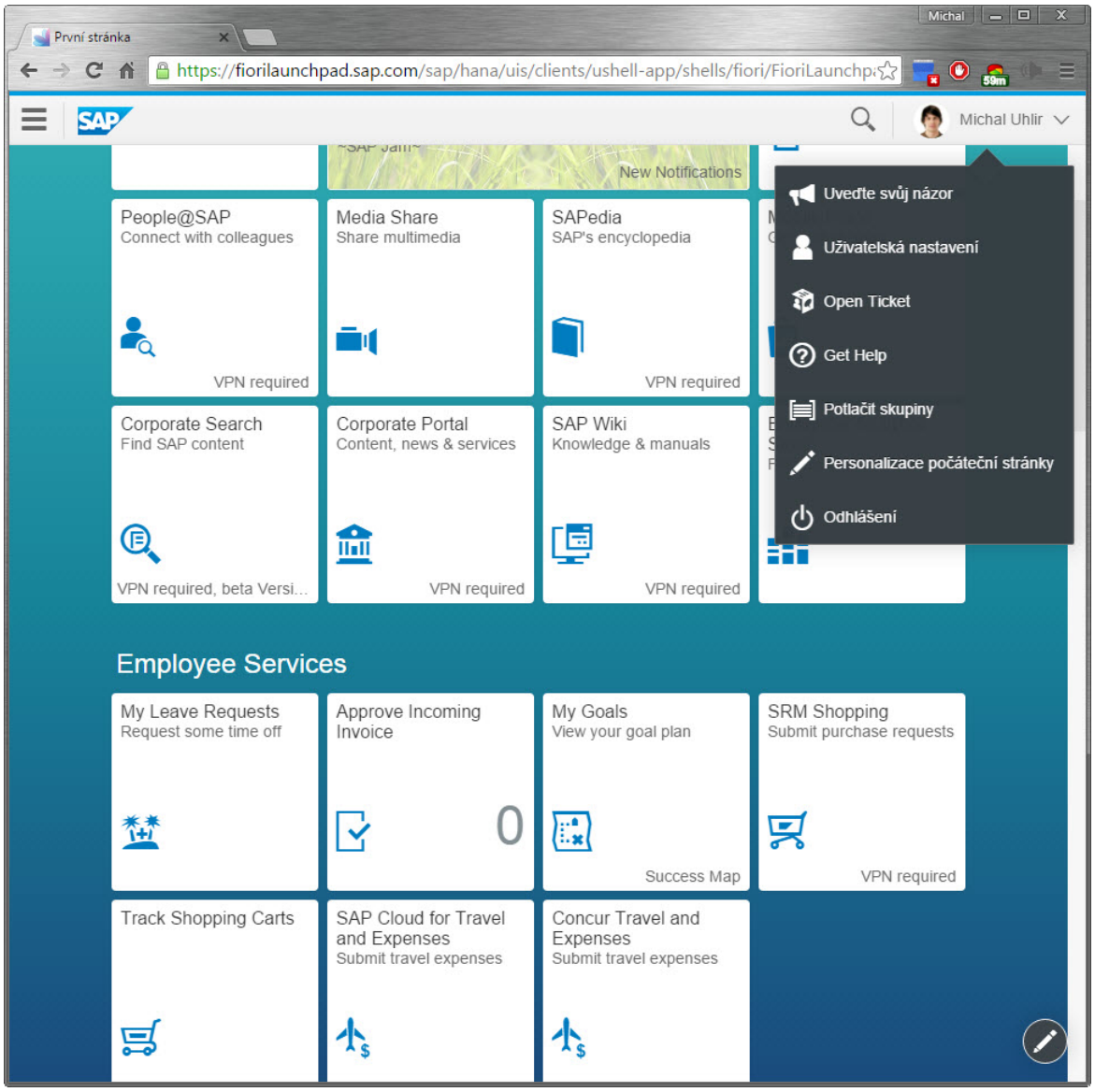


Figure 5.7: SAP Fiori Launchpad.

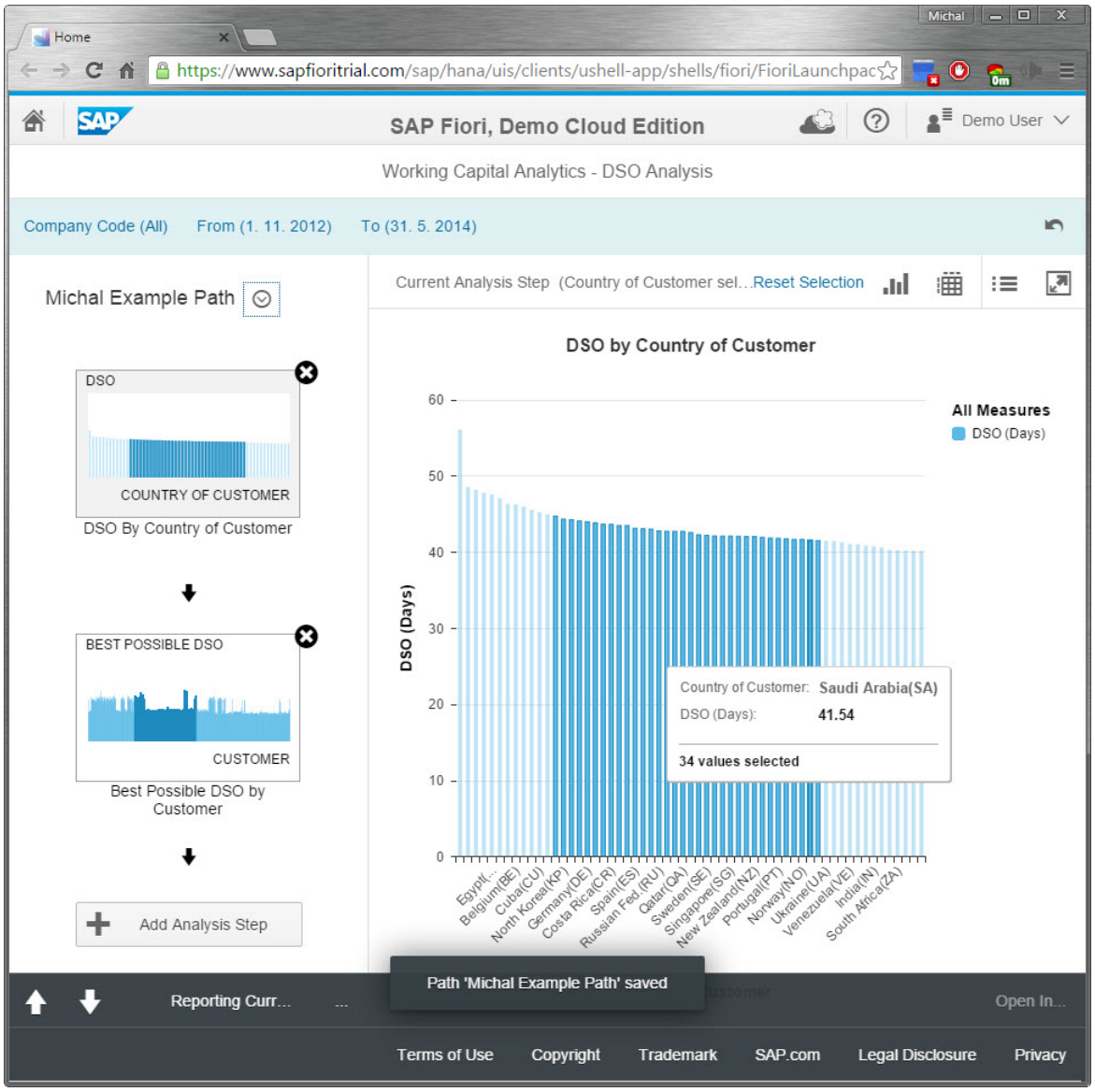


Figure 5.8: Analysis Path Framework example.

Chapter 6

GRC Database Model

In figure 6.2 a simplified data model of SAP GRC can be seen. This model is a basis of an application, which I developed as an object of my thesis. Of course, the standardized version of the SAP software solution is much more complex and the data model is segmented into many various data tables. However, for purposes of this thesis and the developed application only a simplified structure of a few chosen data tables was used. The description below is related to a standard database solution of risk management in SAP.

6.1 Model description

I would start with tables with prefix `HRP`. These are standard tables delivered in HR module of SAP and GRC is using them. Table `HRP1000` is a general table storing the objects like risk, organization unit, or risk category. These objects are time and language dependent and relations between them are stored in the table `HRP1001`.

For clarification see Figure 6.1. In table `HRP1000` we can see three records with different `OBJID`. Field `OTYPE` stands for object type `'OF'` stands for risk object, `'OO'` stands for risk category and `'O '` is used to determine organization unit. If we want to assign risk to organization unit or risk category, this information is stored in table `HRP1001`. Field `OBJID` holds identification of risk and in attribute `SOBID` identification number of risk category or organization unit is stored based on object type in field `SCLAS`.

These objects are time dependent using attributes `BEGDA` and `ENDDA`, determining validity of information. Object details are stored in common `HRP` tables, but for our purpose, it is enough to mention the table `HRP1853` which stores common attributes of risk objects and the table `HRP1846` which is used to store risk attributes. In the table `HRP1002` references to description of object are stored. They are based on validity and its language. Each description is stored in the text table `HRT1002` line by line. Attribute `TABNR` holds identification number of a description, `TABSEQNR` holds sequence number of each line and `TLINE` represents 79 char length text. These tables are mainly connected with 8 digit length object identification `OBJID` and validity attributes `BEGDA` and `ENDDA`. Type of risk is stored in table `GRRMRISKTYPET` under attribute `NAME` and reference field `RISK_TYPE` of table `HRP1930` is used to find the right risk type based also on the language. Client dependency field `MANDT` is a must.

Most important data for final reporting is analysis data stored in the table `GRRMANALYSIS`. This table is a header table of risk analysis, connected with the table of risks by attribute `PARENT_ID`. We store validity, currency or kind of analysis and history of this table is stored

separately in GRRMANALYSIS_TS. Detailed analysis is divided to four tables. GRRMANDATA table is mainly to store probability level and the table GRRMANASSMNT holds data about qualitative impact of risk. The last two tables are used to store information about risk analysis of responses, its effectiveness, probability and completeness in the table GRRMANRESP and qualitative, or quantitative mitigations represented in GRRMANMITIG.

In SAP environment customers can adapt their systems according to their needs. Risk level is stored in the customizing table /ORM/ORMT_RS_L_D as a matrix of probability and impact level. This matrix is determined by a risk level of each risk and its text is stored in the customizing table /ORM/ORMT_RSK_LT.

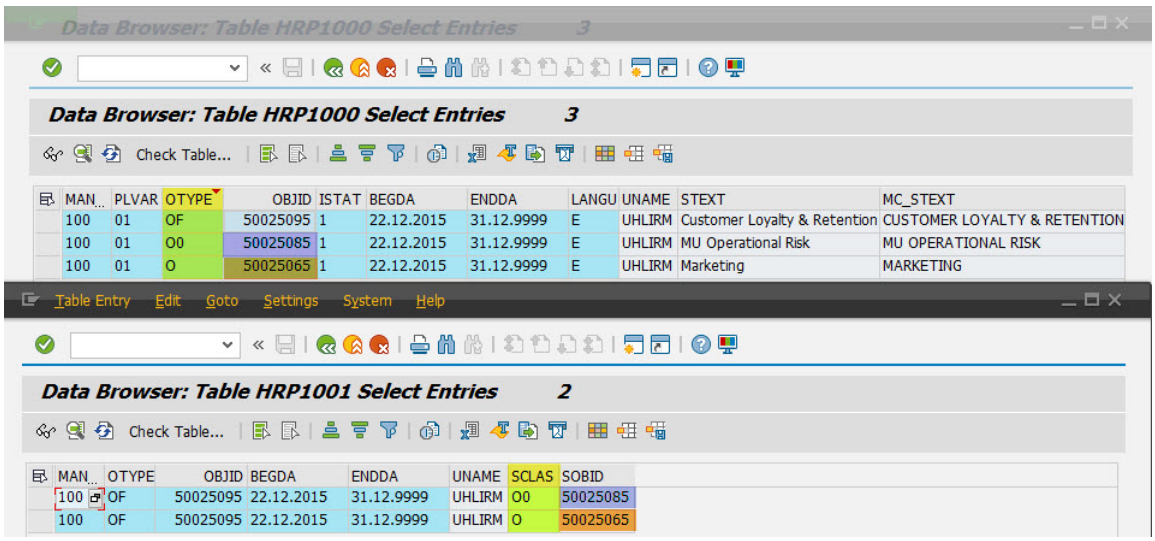


Figure 6.1: HRP1000 and HRP1001 example.

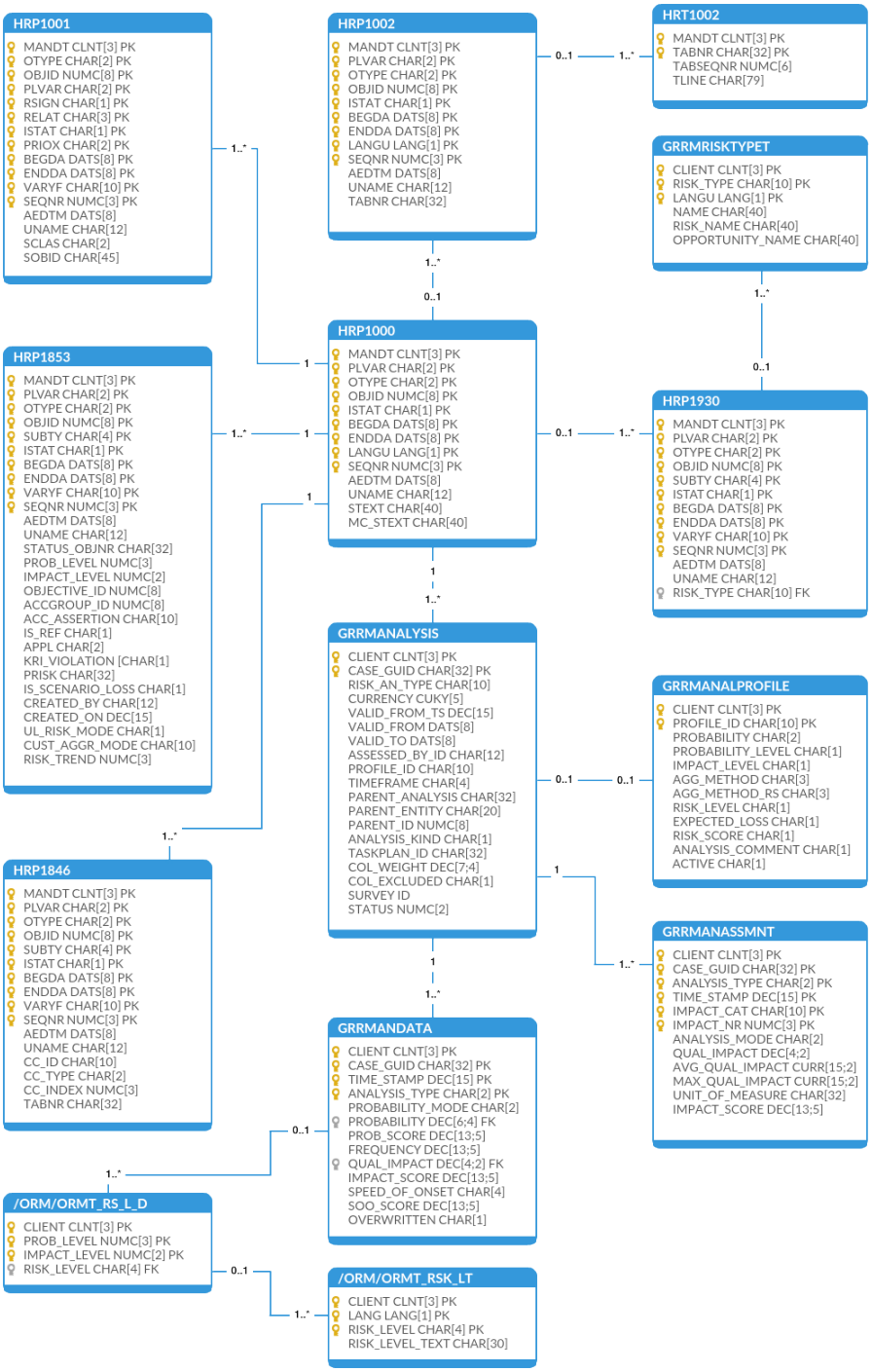


Figure 6.2: GRC Database Model.

Chapter 7

Designed CDS structure

One of the main goals of this thesis is to create a database structure in CDS technology, which is described in section 4.3. This chapter starts with detailed description of CDS views defined in back-end system. By joining particular views, one root view is defined and then used as a basic data model for OData service, which can be consumed by final application through an SAP Gateway. During CDS development I faced some challenges. These unusual issues are summarized at the end of this chapter.

7.1 Definition of CDS views

To get required data from the database, I have created 13 CDS views. Each table B.1 - B.13 contains a description of particular views. Input parameters are widely used to simplify nesting of defined views together. View attributes are presented in the list of fields. Detailed structure of designed model is shown in Figure 7.1.

7.2 Definition of SAP Gateway Service

When data model represented by CDS view is created, next step is to define SAP Gateway Service. In SAP Gateway Service Builder (transaction code `SEGW`) I have created new Gateway Project `ZMU_ANALYSISSERVICE`. The next process step after creating the Gateway Project is to define the project Data Model - in this case I have created the structure by importing it from the DDIC entity – created CDS view. This structure is called Entity Type and based on this, Entity Set is created in the Gateway Project. Then, mapping between the CDS view and the Entity Set is defined. In my case, Entity Set was created from DDIC definition of CDS view, so the mapping of fields could be done automatically. The last step is to create Service Implementation. In this phase, Gateway Model and Data Provider classes are created and the code for the most important methods `GET_ENTITY` and `GET_ENTITIES` are being automatically generated by the framework. Structure of Gateway Project can be seen in Figure 7.2.

To register the newly created Gateway Service within SAP NetWeaver Gateway Hub, SAP transaction code `/IWFND/MAINT_SERVICE` can be used. Testing of created service can be done, for example, from any web browser, or directly from SAP environment. With transaction `/IWFND/GW_CLIENT` we can access a tool called SAP Gateway Client. This tool is mainly used to test Gateway Service by composing HTTP requests and checking returned OData. The way how this tool displays the HTTP response can be seen in Figure 7.3.

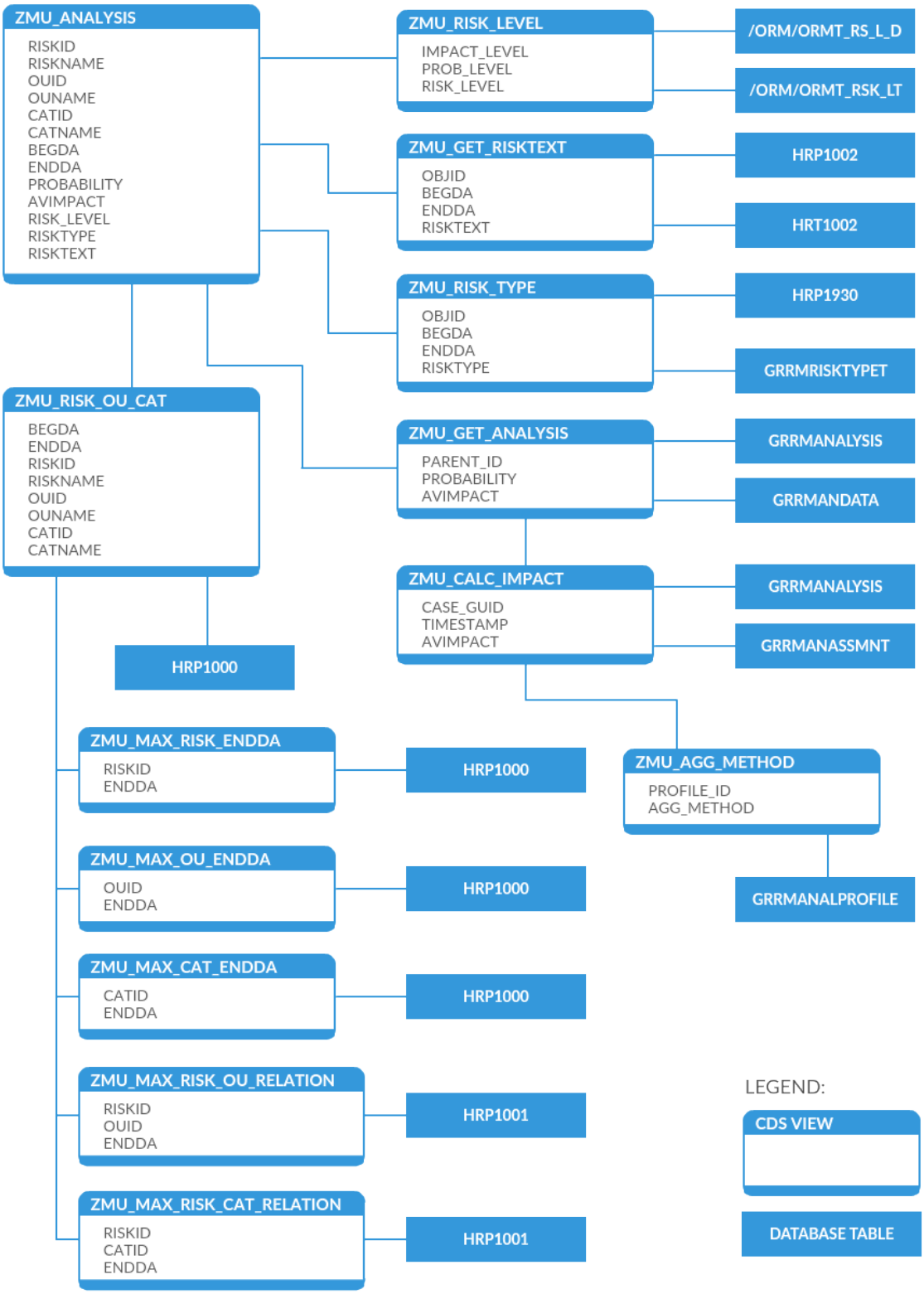


Figure 7.1: Designed CDS structure for CDS.

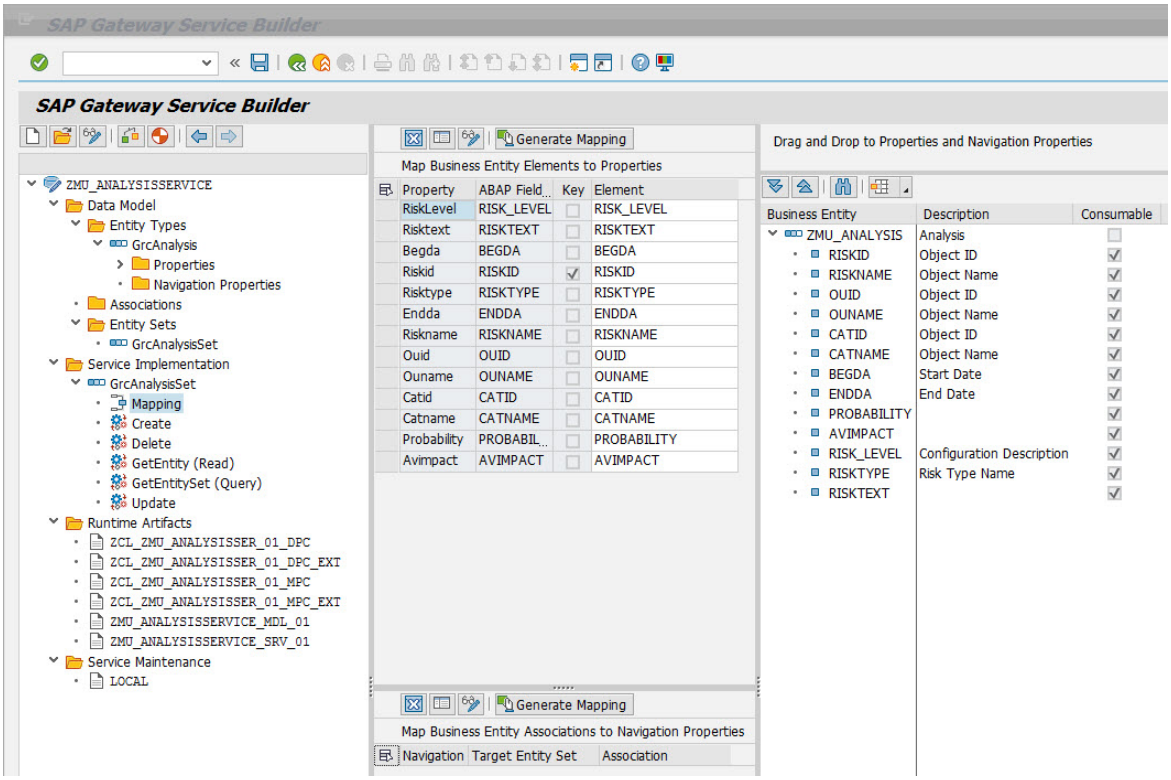


Figure 7.2: SAP Gateway Service Builder screen.

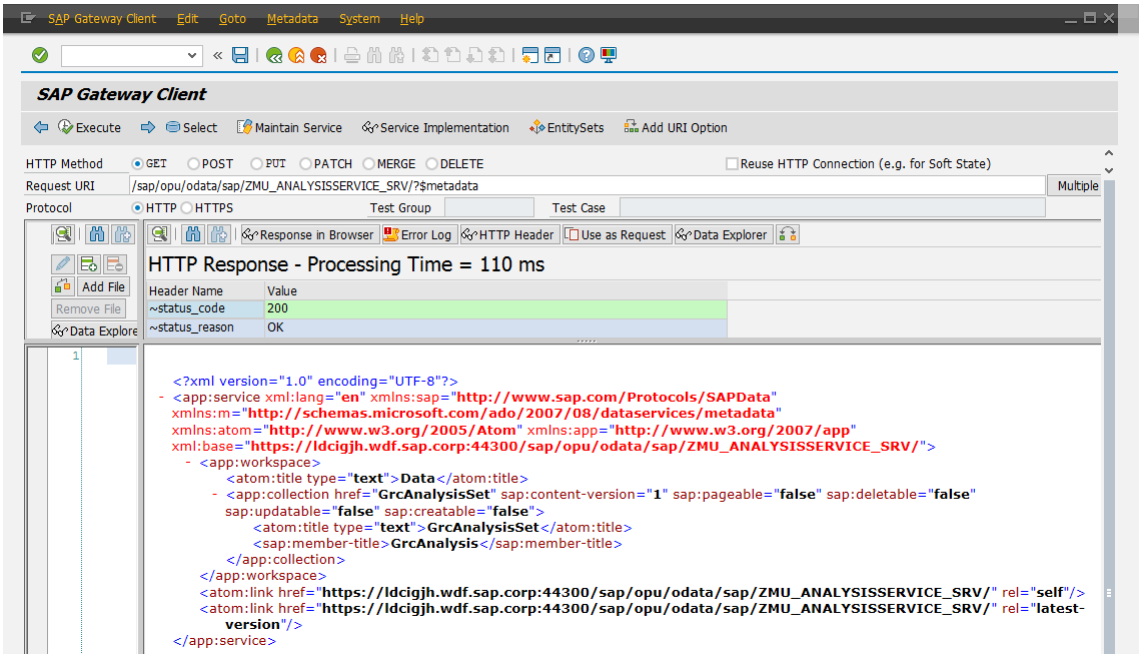


Figure 7.3: SAP Gateway Client.

7.3 Issues

During the development of CDS views, I had to solve some challenging issues. These issues and my solutions are described in the following section more in detail. As already mentioned, all data in SAP GRC solution is time dependent and my solution should follow this feature. The second issue I faced comes with risk description, which is stored in database line by line per 79 chars.

Concept of time dependency in SAP GRC solution is using two attributes for each record - `BEGDA` start of validity, and `ENDDA` end of validity. It means that each risk can have a different name every day. Current GRC reporting applications allow users to define time period for data selection. The first step of selection is to find all data valid in the defined period and then the latest valid record is selected and displayed. Illustrative example, how correct record is selected from the database, can be seen in Figure 7.4.

The second issue to be solved was how to aggregate lines of description into one string. This string can contain HTML tags to format the text that is then displayed to the user. Unlimited number of lines can be stored in the database. To aggregate unknown number of line records CDS technology provides a feature called CDS Table Function, which behaves in the same way as CDS view, but it allows developers to call ABAP class implementing interface `IF_AMDP_MARKER_HDB`. In this class, it is possible to implement logic of selection with SAP HANA SQL Script. With this script language it is possible to use string aggregation function `string_agg`. This function simply concatenate particular strings in required column.

CDS was recently introduced by SAP and development of this feature is still in process. For purpose of my thesis I used GRC development system with internal identification GJD. This system is running with old release ABAP 7.40, but CDS Table Functions are available from release ABAP 7.50. Because of this, my solution is currently selecting only first row from the database. However, I have created example CDS Table Function in sandbox system with newest release and it is ready to be implemented in GJD system after upgrade. Following code demonstrates, how CDS Table Function method is implemented using function `string_agg`.

```
CLASS ZMU_CL_GET_AGGREGATIONS IMPLEMENTATION.
    METHOD GET_TEXT_AGG BY DATABASE FUNCTION FOR HDB
        LANGUAGE SQLSCRIPT
        OPTIONS READ-ONLY
        USING HRT1002.
        RETURN SELECT
                        hrt.mandt as client,
                hrt.tabnr as outputid,
                string_agg(hrt.tline, '') as outline
                FROM HRT1002 as hrt
                                WHERE hrt.mandt = :clnt AND
                        hrt.tabnr = :textid
                GROUP BY hrt.tabnr, hrt.mandt;
    ENDMETHOD.
ENDCLASS.
```

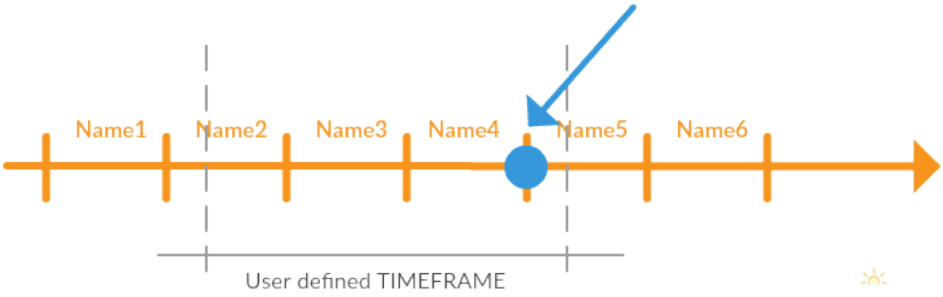


Figure 7.4: Validity concept example.

7.4 Development process

For development of these views, I use Eclipse based development tool called SAP Hana Studio. This work environment integrates different tools to administrate and develop on connected SAP systems. As CDS is completely based on SQL, I declared views in code editor. When view declaration was done, I was able to immediately see the data preview.

At the beginning of development the new structure, I created only one view, which contains complex logic to fetch the data. After discussion with my consultant, I created more simple views and used them as building blocks of final structure. With this approach it would be easier to maintain and overall cleanness of code is increased.

Chapter 8

Validation of designed CDS structure

This chapter contains the description of testing database structure introduced in chapter 7. In first section, Avalon CDS, tool for creation of unit tests in ABAP environment is introduced. Then it is possible to find description of ABAP class developed to validate designed structure. At the end of this chapter, a structure of each test is introduced to get familiar with validation of database structure.

8.1 Avalon CDS

SAP is currently preparing release of Avalon CDS. It is a part of ABAP Unit Test Framework and it enables developers to test the logic expressed in their CDS entities in automated way. It is using the Test Driven Development approach. Tests are represented by a class with keyword `FOR TESTING` which separates this class from the production code. I used this framework many times in past, but to test other functionalities of ABAP - not for CDS structures. The program code and the test code share the same life cycle and are always synchronized. The test code can validate the program code but not vice versa. The release was planned for February 2016, but due to some internal issues, it is still not released and could have not be used for the testing purposes of this thesis. As this framework is not available, I decided to implement my own class to test the functionality of designed CDS views. My implementation is described below.

8.2 Test class implementation

To test designed CDS structure described in chapter 7 I have created a new ABAP class `ZMU_GRCANALYSIS_TEST`. It can be executed from SAP Workbench transaction code `SE80` or directly from ABAP Class Builder calling transaction code `SE24`. This class contains implementation of methods to test each particular view. Mapping of methods and tested views is clearly shown in Table 8.2. These tests can be executed one by one or all together by method `RUN_ALL`. This method executes all the tests and provides output of results on screen. All methods are implemented as `static` with `public` visiblility.

Method	Tested CDS view
TEST1	ZMU_MAX_ANALYSIS_ENDDA
TEST2	ZMU_MAX_CATEGORY_ENDDA
TEST3	ZMU_MAX_OU_ENDDA
TEST4	ZMU_MAX_RISK_CAT_RELATION
TEST5	ZMU_MAX_RISK_ENDDA
TEST6	ZMU_MAX_RISK_OU_RELATION
TEST7	ZMU_RISK_TYPE
TEST8	ZMU_AGG_METHOD
TEST9	ZMU_CALC_IMPACT
TEST10	ZMU_RISK_LEVEL
TEST11	ZMU_RISK_OU_CAT
TEST12	ZMU_ANALYSIS

Table 8.1: Mapping of test method and tested CDS view.

8.3 Test structure

Structure of each method TEST1 - TEST12 is following the same pattern for testing, if CDS view is fetching data properly from database tables. At the beginning of the test, data is selected from tested CDS view and stored in internal table `CDS_RESULT`. The second internal table `LT_ABAP_RESULTS` is filled with data using standard ABAP statements, but with the same logic. Two checks are performed, when both internal tables are loaded. The first check is to determine, if both tables have the same number of lines. If this check is successful, it goes through table lines in table `LT_ABAP_RESULTS` and searches for the line with the same data in table `CDS_RESULT`. Return value of this method is of type `CHAR` with length 1, which is used in SAP to implement type boolean. Value "true" is defined as `'X'` and value "false" is defined as `' '` also known as `space`.

These tests are created only to validate that defined CDS view is selecting data accordingly. To test the performance of newly created views I would need huge of test data, which is not possible to achieve in SAP development system.

8.4 Test data

For testing purpose not only back-end development I created test data as user of GRC environment. It is not possible to create test data by SQL script, because the database structure of whole GRC is huge, I would not be able to insert data to all necessary tables, and I would definitely create inconsistencies.

When developing front-end of application in WebIDE, it is possible to create mock data based on structure of consumed data model and randomly generate its values, or define own. I created mock data to test my application when SCC is not connected to on-premise system, but it make no sense to generate random data so I manually filled it with data provided by created service.

Chapter 9

Application for risk management reporting

Current SAP GRC solution introduced in section 3.1. provides many reports for end users, but these reports are built by using old technologies such as ABAP Dynpro (5.1), or ABAP Web Dynpro (5.2). The main goal of this part was to analyze new UI technologies and create prototype of risk reporting application. With my consultant, we identified APF and SAPUI5 library as suitable technologies for creation of this type of application.

The only limitation for our decision was to stay with SAP technologies. Main reason for this decision is that SAP is now presenting SAP Fiori technologies as future way of SAP user interface and every development department should be able to step by step develop its application in this technology. These applications can be executed on mobile devices, which would be appreciated by GRC customers. We have chosen APF framework, because it is focused on analytics reports and can be easily extended by its users. Every user can create own analysis path with provided chart types.

This chapter is focused on technologies used to develop the reporting application, such as SAPUI5, SAP HANA Cloud Connector and OData Services. In section 9.1 I described a reason, why I did not use APF. At the end of this chapter, advantages and disadvantages of SAPUI5 for GRC reporting are mentioned.

The main reason, why I decided to use HCP, described in section for front-end development was internal processes at SAP. The configuration of front-end development environment was not ready on development system and it would take some time and I could got stuck in similar way as with APF configuration. In cloud based HCP, all services are up to date and ready to be used by developers or users.

As my application is running in HCP and data is stored in on-premise development system, I used SCC to configure the connection. Firstly users have to install the Cloud connector into their device. The next step is to set up mutual authentication between the Cloud connector and a back-end system. By configuration of HTTP access control, it is possible to allow the cloud application to access a back-end system on the intranet.

9.1 Usage of APF

At the beginning of this part, I decided to use APF, described in 5.6.4 to develop the application. This framework allows end user to extend delivered application and analyze own risk data according to the business needs. It was recently introduced as a new feature

of SAP Fiori. Because of the fact that this technology is quite raw, I was not able to get working installation of this framework on our development system. Its installation is still in progress with many colleagues involved. After the discussion with my supervisor and consultant, we decided not to use APF as part of this thesis.

9.2 Open Data Services (OData)

OData is based on Representational State Transfer (REST) architecture and helps you to focus on your business logic while building APIs without worrying how to define request and response headers, HTTP methods, status codes, media types, URL conventions, or query options. As common practices of REST, OData is using HTTP, AtomPub and JSON to address and access data resources. It guides the user through the definition of functions for reusable procedures and passing batch or asynchronous requests. OData APIs are easy to consume by applications. Metadata, a machine readable description of the data structure enables the creation of complex generic tools and client proxies. It can help you to interact with OData without a deep knowledge of the protocol. [12]

As mentioned in section 7.2, OData Service is used to exchange data between back-end system and front-end application. This service is active in back-end system GJD and it is ready to use. It is possible to get XML output directly from web browser, or consume the data by any web application. It is possible to access this data using APF. In case of developed application, this service is used as base data model.

9.3 SAP Splash and BUILD

SAP Splash and BUILD are integrated cloud-based tools constructed to address the critical Design and Discovery phases of the product lifecycle.

SAP SPLASH enables development teams to design software experiences by providing them with learning content on design thinking practices. It contains a gallery of well designed applications that can serve as an inspiration and can be leveraged at the beginning of the design process. It is possible to follow e-Learning about design thinking methodologies, best practice guidelines and use the templates. [7]

When project is designed using SAP SPLASH, logical next step is to use collaborative design tool **BUILD** to create interactive prototype that can be shared with users. It is possible to use imported mockups, introduced in subsection 5.6.2, to add own sample data. With integrated research and analytic tools it is easy to gather effective user feedback. When this process is finalized, BUILD can generate SAPUI5 source code to easier start of development process. [7]

I found these tools very helpful at the beginning of the design process, when I did not have deeper knowledge of SAPUI5 library and I wanted to discuss functionality with other colleagues and my consultant. It is easy to use and the user is able to create prototype of any application in a short time.

9.4 Heatmap prototype

In Figure 9.1 the screen of heatmap report created in ABAP Web Dynpro technology described in section 5.2 can be seen. This kind of GRC report shows number of risks categorized by probability and impact level. The detail of each risk can be accessed by clicking

to the risk name. Data can be filtered by timeframe or organizational unit. It provides also some other filtering possibilities, but these are not commonly used by customers.

As part of this thesis, I have created a similar report using SAPUI5 library. This prototype application consumes data model, which is described in chapter 7 through OData Service. This was completely developed in HCP described in section 9 using web browser based development tool WebIDE introduced in subsection 5.6.2.

The main screen of the application is very similar to the old report and can be seen in Figure 9.2. As filter criteria it is sufficient to use organization unit and time period. Based on the discussion with SAP consultants, I decided to use time period represented by start date and end date. In the old report it was only possible to filter data per year. Heatmap chart is displayed as table with different background color of cells. The last object on this screen is a list of risks. From this list, the user can navigate to the risk detail to see description of particular risk. It is possible to search for risk by name. The risk detail screen is displayed in Figure 9.3. This application is following SAP Fiori Design Guidelines [5].

9.5 Application development in WebIDE

As mentioned in introduction of this chapter, development of final application was done in HCP using WebIDE. This tool allows developer to create own application from scratch or use one of the predefined template. Templates primarily to show developers kind of best practice usage of SAPUI5 library controls. Third possibility is to import basic structure of designed application straight from BUILD tool described in 9.3. I have chosen this way of creation of new application and it helped me to create XML structure of windows, but I have to define many controls manually. My application is based on well known MVC architecture.

Model is represented by OData service described in section 7.2. **View** is represented by XML structure and it is mainly edited by code editor, because graphic WYSIWYG editor does not support all controls and the performance of graphical editor is not so high. Logic of **controller** is written in Javascript and no code is generated when user add control via graphic editor. Each window of my application is represented by own view and controller file.

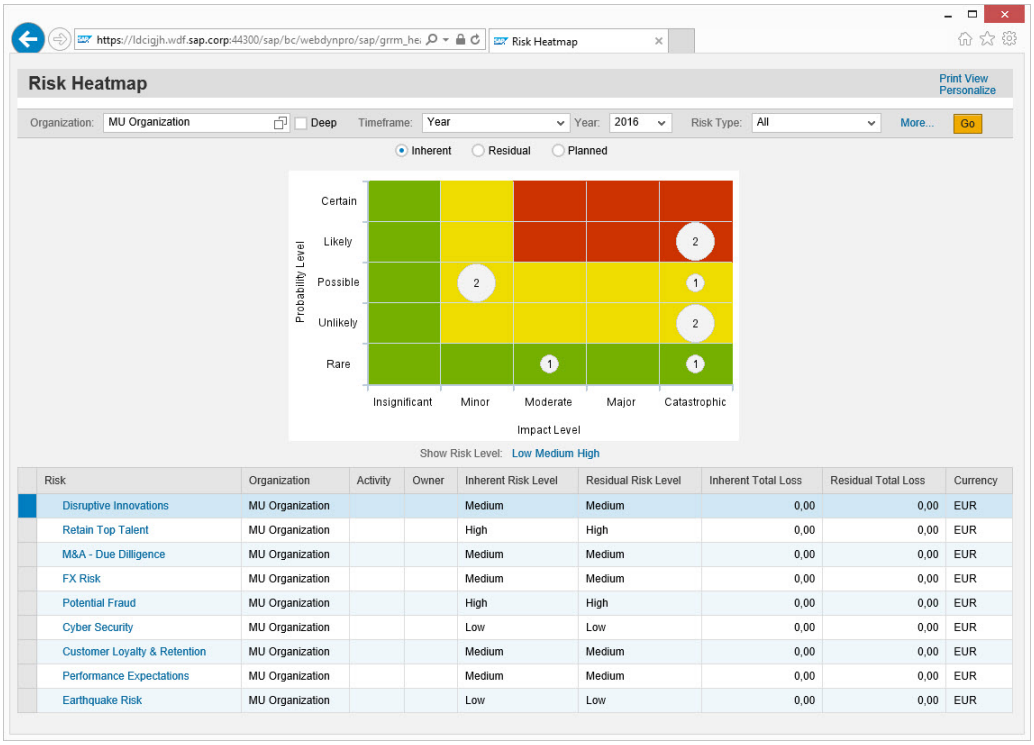
9.6 Advantages and Disadvantages of SAPUI5

In this section, I analyze advantages and disadvantages of using SAPUI5 for GRC reporting. All applications created with SAPUI5 support cross platform execution. Users can run these applications on desktop or mobile devices. It is very easy to extend SAPUI5 applications, or change the theme of this application with SAP UI Theme Designer mentioned in section 5.5.

Using this concept data is consumed in real time and no preprocessing of data have to be executed. The user is able to react to current data in his system. SAPUI5 is now dominating technology for innovation of whole SAP environment and GRC also needs to react to this new feature. Accessing GRC applications can be much faster from SAP Fiori Launchpad 5.6.3, which is easy to run and use. For the future development it is also very important, that these applications are role based and user can use SAPUI5 applications only when necessary role is assigned to his account.

SAPUI5 library is very well documented and many examples are provided for users to better understand, how to implement any part of it. When an application is designed by development team from scratch with cooperation of end users, it is very helpful to use integrated tools SAP Splash and BUILD.

When I think about disadvantages, I have to mention that all technologies are quite new and new releases comes very fast with new features and bug fixes. Therefore it is sometimes hard to stay oriented. It will take some time to get these technologies, for example WebIDE, more stable to work with. As I have chosen to develop in HCP, I have to be always online and connected to internet.



Risk	Organization	Activity	Owner	Inherent Risk Level	Residual Risk Level	Inherent Total Loss	Residual Total Loss	Currency
Disruptive Innovations	MU Organization			Medium	Medium	0,00	0,00	EUR
Retain Top Talent	MU Organization			High	High	0,00	0,00	EUR
M&A - Due Dilligence	MU Organization			Medium	Medium	0,00	0,00	EUR
FX Risk	MU Organization			Medium	Medium	0,00	0,00	EUR
Potential Fraud	MU Organization			High	High	0,00	0,00	EUR
Cyber Security	MU Organization			Low	Low	0,00	0,00	EUR
Customer Loyalty & Retention	MU Organization			Medium	Medium	0,00	0,00	EUR
Performance Expectations	MU Organization			Medium	Medium	0,00	0,00	EUR
Earthquake Risk	MU Organization			Low	Low	0,00	0,00	EUR

Figure 9.1: ABAP Web Dynpro Heatmap.

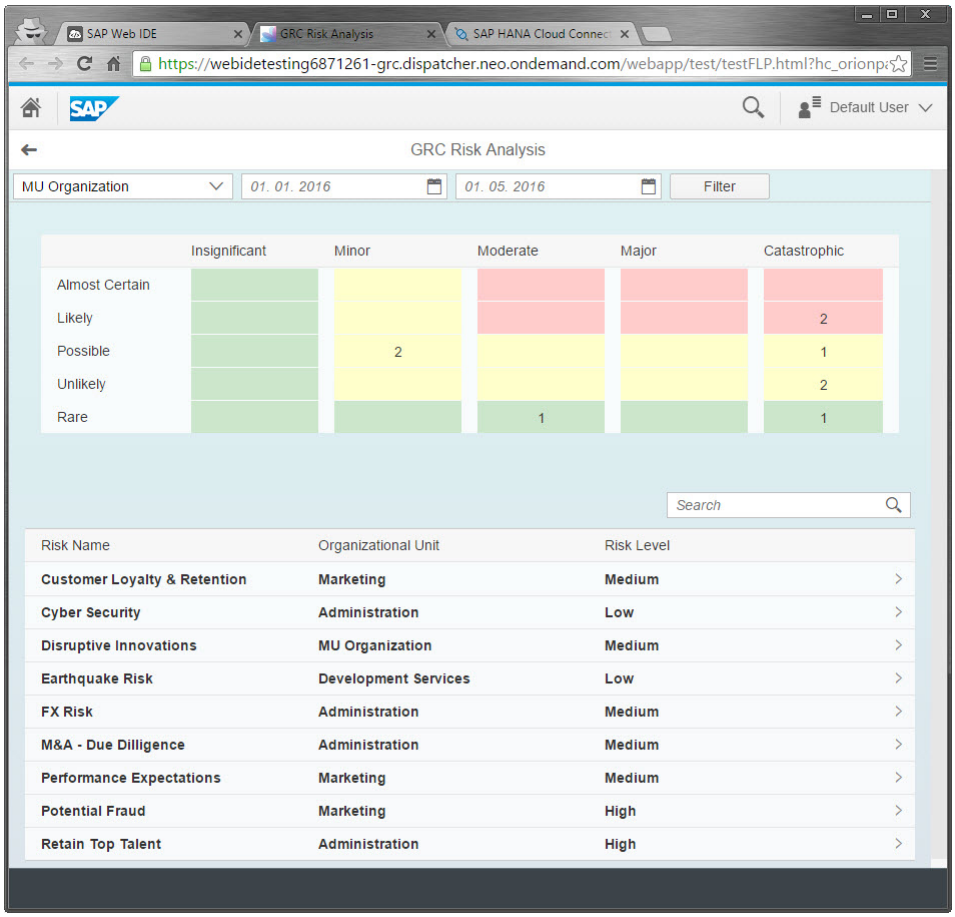


Figure 9.2: SAPUI5 Heatmap report.

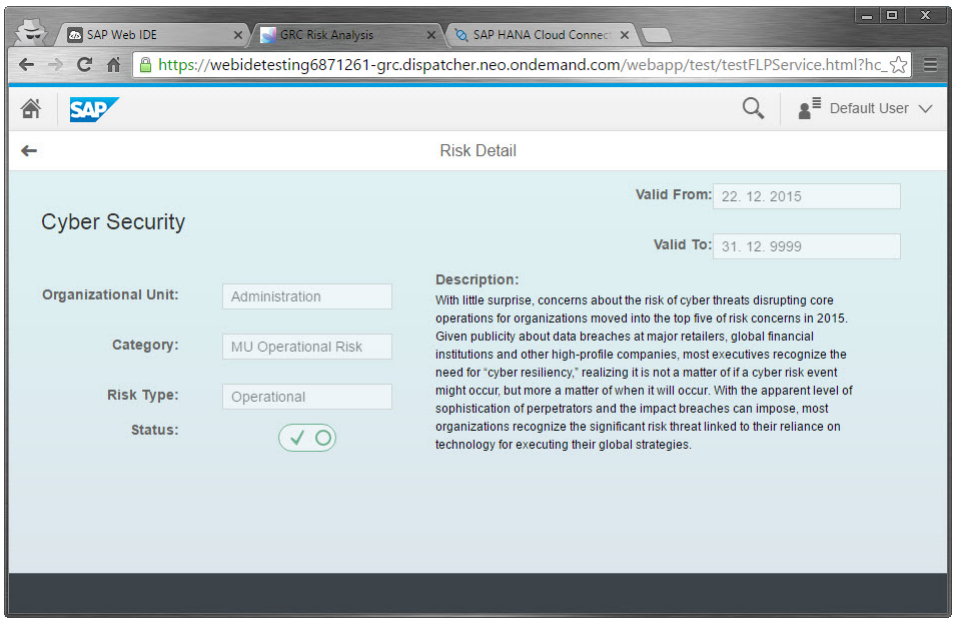


Figure 9.3: SAPUI5 Risk Detail.

Chapter 10

Conclusion

The first task for this thesis was to get acquainted with risk management in companies. By studying various sources dealing with GRC topics I identified key principles of the concept and GRC processes and activities that are being performed in organizations. It was an interesting part of the task to analyze and compare available GRC software solutions. It helped me to understand better the purpose of my application, so I was able to design it accordingly.

I studied deeply latest SAP technologies to get an overview of what is currently available and what could be useful for development of my application. Then I focused on the SAP GRC solution and its database structure that I analyzed in detail in order to get an idea of how my data model could be organized. When I set up the data model, proper validation was needed. For this purpose I wanted to use framework for Unit testing of standard ABAP objects, but as this framework is not available for CDS technology, I decided to create my own test class.

After the back-end of the application was finalized I designed and developed the user interface. Final application is developed in HCP, which is connected via SCC to the back-end development system. This application is developed by using SAPUI5 library, which is a new technology for creation web based responsive applications. Comparison of advantages and disadvantages could be very helpful for future decision, what technology could be used for GRC development in SAP.

As the APF framework was not available before I finished this thesis, the future work will be to analyze APF for GRC reporting and configure this framework to display the data provided by created OData service.

Bibliography

[1] *EMC PULSE: Product & Technology Blog.* [online]. 2014 [cit. 2016-05-17]. Retrieved from: http://pulseblog.emc.com/2014/11/10/emc-rsa-leader-inaugural-gartner-magic-quadrant-vendor-risk-management/.

[2] *IT Convergence: Oracle Fusion Applications Webcast Q&A Part II.* [online]. 2016 [cit. 2016-05-17]. Retrieved from: http://www.itconvergence.com/blog/oracle-fusion-faqs-fusion-applications/.

[3] *Open Pages and the convergence of Performance Management.* [online]. [cit. 2016-05-17]. Retrieved from: http://www.performance-ideas.com/2011/09/27/grc-erwin-boeren/.

[4] *RSA Archer GRC - Governance, Risk and Compliance: Solution Overview.* [online]. 2016 [cit. 2016-05-17]. Retrieved from: https://www.emc.com/collateral/solution-overview/h13430-rsa-archer-grc-pb.pdf.

[5] *SAP Fiori Design Guidelines.* [online]. [cit. 2016-05-17]. Retrieved from: https://experience.sap.com/fiori-design/.

[6] *SAP HANA Cloud Connector.* [online]. [cit. 2016-05-17]. Retrieved from: https://hcp.sap.com/capabilities/integration/hana-cloud-connector.html.

[7] *SAP Splash and BUILD.* [online]. [cit. 2016-05-17]. Retrieved from: https://hcp.sap.com/capabilities/ux/build-splash.html.

[8] *UI Development Toolkit for HTML5 (SAPUI5).* [online]. [cit. 2016-05-23]. Retrieved from: https://help.sap.com/saphelp_uiaddon10/helpdata/en/95/d113be50ae40d5b0b562b84d715227/content.htm.

[9] ADAMS, Sarah, Carlos RUIZ and Elias Rivera: *Governance, Risk and Compliance.* [online]. May 2013 [cit. 2016-05-10]. Retrieved from: http://www.isaca.org/chapters7/Monterrey/Events/Documents/20132305 Governance, Risk and Compliance.pdf.

[10] BAINBRIDGE, Stephen M: *The complete guide to Sarbanes-Oxley: understanding how Sarbanes-Oxley affects your business.* Adams Media, 2007, iSBN 9781598692679.

[11] BAVARAJU, Anil: *SAP fiori implementation and development.* Rheinwerk Publishing, SAP PRESS, 2016, iSBN 9781493212484.

[12] BONNEN, Carsten: *OData and SAP NetWeaver Gateway.* Boston: Galileo Press, 2014, iSBN 9781592299096.

[13] Deloitte: *Exploring Strategic Risk: 300 executives around the world say their view of strategic risk is changing*. [online]. 2013 [cit. 2016-05-04]. Retrieved from: http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-exploring-strategic-risk.pdf.

[14] Governance, Risk and Compliance Framework: *MetricStream*. [online]. [cit. 2016-05-04]. Retrieved from: http://www.metricstream.com/whitepapers/html/GRC_frame.htm.

[15] KIRKPATRICK, Grant. The Corporate Governance Lessons from the Financial Crisis.: *Financial Market Trends*. [online]. 2009 [cit. 2016-05-03]. ISSN 1995-2864. Retrieved from: http://www.oecd.org/daf/ca/corporategovernanceprinciples/42229620.pdf.

[16] Klitscher, A.: *Finanzielles Riskomanagement als zentrale Aufgabe des Treasurers SAP Financial Excellence Forum 2013 11. April 2013*. [online]. 2013 [cit. 2016-05-17]. Retrieved from: http://docplayer.net/3827889-Finanzielles-riskomanagement-als-zentrale-aufgabe-des-treasurers-sap-financial-excellence-forum-2013-11-april-2013.html.

[17] PLATNER, Hasso: *A Course in In-Memory Data Management*. New York: Springer, 2013, iSBN 9783642365232.

[18] SABINE SCHÖLER, Olaf Zink: *SAP governance, risk and compliance*. Boston: Galileo Press, 2009, iSBN 9781592291915.

[19] SAP AG: *Access Control 10.1: Master Guide. 2013*. Retrieved from: https://websmp205.sap-ag.de/šapidb/011000358700000596312013E.

[20] SAP AG: *SAP Global Trade Services*. [online]. 2016 [cit. 2016-05-17]. Retrieved from: http://go.sap.com/product/analytics/global-trade-management.html.

[21] TERO, Vivian: *The case for GRC: Addressing the TOP 10 GRC Challenges*. [online]. 2012 [cit. 2016-05-04]. Retrieved from: https://www.rsa.com/content/dam/rsa/PDF/h11523-idc-case-for-grc-addressing-top-10-challenges.pdf.

[22] The Committee of Sponsoring Organizations of the Treadway Commission: *Enterprise Risk Management — Integrated Framework: Executive Summary*. [online]. 2004 [cit. 2016-05-04]. Retrieved from: http://www.coso.org/documents/coso_erm_executivesummary.pdf.

[23] UHLÍŘ, Michal: *SAP HANA Platform*. Brno, 2014. Bachelor's thesis. Brno University of Technology, Faculty of Information Technology. Supervisor Zendulka Jaroslav. Retrieved from: http://www.fit.vutbr.cz/study/DP/BP.php?id=16555.

[24] Vanderbilt University: Office of Internal Audit and Institutional Risk Management: *Are there Different Types of Internal Controls?* [online]. [cit. 2016-05-04]. Retrieved from: https://www4.vanderbilt.edu/internalaudit/internal-control-guide/different-types.php.

[25] VU BROADY, Denise and Holly A. ROLAND: *SAP GRC for dummies*. Hoboken, NJ: Wiley, iSBN 9781598692679.

[26] WOOD, James: *Getting started with SAP HANA Cloud Platform*. Boston: Rheinwerk Publishing, 2015, iSBN 9781493210213.

[27] WOOD, James and Shaan. PARVAZE: *Web Dynpro ABAP: the comprehensive guide*. Galileo Press, 2013, iSBN 1592294162.

Appendices

List of Appendices

Appendix A

Content of CD

- `thesis` - source files for LaTeXof this thesis
  - `img` - figures
- `source` - source code of created views, tests and final applications
  - `application` - source code of front-end application
  - `CDS views` - source code of defined CDS views
  - `Test class` - source code of test class

Appendix B

View Descriptions

ZMU_ANALYSIS	**Input parameters:** BEGDA, ENDDA
Fields: RISKID RISKNAME OUID OUNAME CATID CATNAME BEGDA ENDDA PROBABILITY AVIMPACT RISK_LEVEL RISKTYPE RISKTEXT	**Description:** The main view of designed data model. It contains all required attributes and it is used to define OData service, which is consumed by final application. Unique field of this view is always `RISKID` and other fields are filled with related information. Input parameters `BEGDA` and `ENNDA` are defined because of time dependency of the whole concept. It is discussed later in this chapter. For testing purposes, these parameters are set to default values and not used.

Table B.1: ZMU_ANALYSIS

ZMU_RISK_OU_CAT	**Input parameters:** BEGDA, ENDDA
Fields: RISKID RISKNAME OUID OUNAME CATID CATNAME BEGDA ENDDA	**Description:** This view selects required risks and related organization unit, category and time dependency of this risk. As these objects are time dependent and all of them are stored in table `HRP1000`, this view contains definition of join of nested views and passes input parameters to them.

Table B.2: ZMU_RISK_OU_CAT

ZMU_MAX_RISK_ENDDA	**Input parameters:** BEGDA, ENDDA
Fields: RISKID ENDDA	**Description:** Selection of all risks valid in the time period defined by input parameters from table `HRP1000`.

Table B.3: ZMU_MAX_RISK_ENDDA

ZMU_MAX_OU_ENDDA	**Input parameters:** BEGDA, ENDDA
Fields: OUID ENDDA	**Description:** Selection of all organization units valid in the time period defined by input parameters from table `HRP1000`.

Table B.4: ZMU_MAX_OU_ENDDA

ZMU_MAX_CAT_ENDDA	**Input parameters:** BEGDA, ENDDA
Fields: CATID ENDDA	**Description:** Selection of all risk categories valid in the time period defined by input parameters from table `HRP1000`.

Table B.5: ZMU_MAX_CAT_ENDDA

ZMU_MAX_RISK_OU_RELATION	**Input parameters:** BEGDA, ENDDA
Fields: RISKID OUID ENDDA	**Description:** Selection of all risk and organization unit relations valid in the time period defined by input parameters from table `HRP1001`.

Table B.6: ZMU_MAX_RISK_OU_RELATION

ZMU_MAX_RISK_CAT_RELATION	**Input parameters:** BEGDA, ENDDA
Fields: RISKID CATID ENDDA	**Description:** Selection of all risk and category relations valid in the time period defined by input parameters from table `HRP1001`.

Table B.7: ZMU_MAX_RISK_CAT_RELATION

ZMU_RISK_LEVEL	
Fields: IMPACT_LEVEL PROB_LEVEL RISK_LEVEL	**Description:** Risk level is selected based on `IMPACT_LEVEL` and `PROB_LEVEL` from table `/ORM/ORMT_L_D`. SAP usually stores text in special tables, because of language dependency. Risk level text is selected from table `/ORM/ORMT_RSK_LT`.

Table B.8: ZMU_RISK_LEVEL

ZMU_GET_RISKTEXT	**Input parameters:** BEGDA, ENDDA
Fields: OBJID BEGDA ENDDA RISKTEXT	**Description:** Risk text ID is selected from table `HRP1002` based on input parameters `BEGDA` and `ENDDA`. As text is divided to lines per 79 chars, table function with parameters is created to get data from text table `HRT1002`. This process is described in section 7.3.

Table B.9: ZMU_GET_RISKTEXT

ZMU_RISK_TYPE	
Fields: OBJID BEGDA ENDDA RISKTYPE	**Description:** Risk type ID is selected from table `HRP1930` based on system language and text field is selected from GRC text table `GRRMRISKTYPET`.

Table B.10: ZMU_RISK_TYPE

ZMU_GET_ANALYSIS	**Input parameters:** ENDDA
Fields: PARENT_ID PROBABILITY AVIMPACT	**Description:** Field `PARENT_ID` of table `GRRMANALYSIS` is connector to field `OBJID`, ID of risk. Attribute `PROBABILITY` is selected from table `GRRMANDATA`.

Table B.11: ZMU_GET_ANALYSIS

ZMU_CALC_IMPACT	
Fields: CASE_GUID TIMESTAMP AVIMPACT	**Description:** Field `AVIMPACT` is calculated from field `QUAL_IMPACT` of table `GRRMANASSMNT` by method selected from view `ZMU_AGG_METHOD`.

Table B.12: ZMU_CALC_IMPACT

ZMU_AGG_METHOD	
Fields: PROFILE_ID AGG_METHOD	**Description:** Aggregation method (MAX,AVG,SUM) is selected from table `GRRMANALPROFILE` based on attribute `PROFILE_ID`.

Table B.13: ZMU_AGG_METHOD