FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

ASSIGNMENT OF MASTER’S THESIS

Title:	Model-Driven Approach to Governance, Risk, and Compliance Systems Development
Student:	Bc. Martin Mužák
Supervisor:	Ing. Marek Skotnica
Study Programme:	Informatics
Study Branch:	Web and Software Engineering
Department:	Department of Software Engineering
Validity:	Until the end of summer semester 2019/20

Instructions

Governance, Risk and, Compliance (GRC) plays a very important role in state-of-the-art enterprises. In the report "Speed of business", it was estimated that companies spend on average 6% of their expenses on the compliance alone.
A goal of this thesis is to investigate how model-driven systems can help companies with the GRC management to reduce their operating costs.

Steps to take:

- Review the state of the art GRCplatforms.
- Compare the benefits and suitability ofGRC platforms, BPM systems, Low-code platforms, and custom development tosupport GRC management.
- Propose a suitable software architecturefor implementing a GRC system.
- Create a case study which willdemonstrate an implementation of a model-driven GRC system in an enterprise.

References

Will be provided by the supervisor.

Ing. Michal Valenta, Ph.D.
Head of Department

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
Dean

Prague November 7, 2018

FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Master’s thesis

Model-Driven Approach to Governance, Risk and Compliance Systems Development

Bc. Martin Mužák

Department of Software Engineering Science
Supervisor: Ing. Marek Skotnica

April 29, 2019

Acknowledgements

I would like to thank my supervisor Ing. Marek Skotnica for introducing me to this interesting topic, as well as for his support during the development process and writing of this thesis. Also, I would like to thank my family and friends for all their support during my studies.

Declaration

I hereby declare that the presented thesis is my own work and that I have cited all sources of information in accordance with the Guideline for adhering to ethical principles when elaborating an academic final thesis.

I acknowledge that my thesis is subject to the rights and obligations stipulated by the Act No. 121/2000 Coll., the Copyright Act, as amended. I further declare that I have concluded an agreement with the Czech Technical University in Prague, on the basis of which the Czech Technical University in Prague has waived its right to conclude a license agreement on the utilization of this thesis as school work under the provisions of Article 60(1) of the Act. This fact shall not affect the provisions of Article 47b of the Act No. 111/1998 Coll., the Higher Education Act, as amended.

In Prague on April 29, 2019 ....

Czech Technical University in Prague
Faculty of Information Technology

Citation of this thesis

Mužák, Martin. *Model-Driven Approach to Governance, Risk and Compliance Systems Development.* Master's thesis. Czech Technical University in Prague, Faculty of Information Technology, 2019.

Abstract

This Master's thesis is devoted to the model-driven approach to governance, risk and compliance systems development. GRC systems are discussed in detail and these systems are compared to BPM systems and low-code platforms. Moreover, software architecture is described and one specific implementation is proposed. To demonstrate the usability of GRC systems, one of the bank processes, money-laundering payment recognition, is created in BPMN and deployed via the workflow engine Camunda.

Keywords GRC, Governance, Risk, Compliance, software architecture, Camunda, BPMN, bank processes, money-laundering, BPM

Abstrakt

Tato magisterská práce se věnuje modelem řízenému přistupu pro vývoj systémů pro governance, risk a compliance. Podrobně je diskutována problematika GRC systémů a tyto systémy jsou porovnávány s BPM systémy a low-code platformami. Následně je popsána softwarová architektura a navržen jeden konkrétní přístup implementace. Pro demonstraci použitelnosti systémů GRC je v BPMN vytvořen bankovní proces – rozpoznávání plateb pro praní špinavých peněz a tento model je nasazen do systému Camunda.

Klíčová slova GRC, Governance, Risk, Compliance, Camunda, softwarová architektura, BPMN, bankovní procesy, praní peněz, BPM

Contents

List of Figures

Introduction

Motivation and Objectives

It is estimated that companies will spend over 6%[1] of their annual turnover just to comply with regulations. In order to fulfill all the requirements presented by different authorities, be it local governance, international union or state bank, companies have to spend a huge amount of their resources just to be compliant. To be compliant in the world, where law or regulation changes irregularly bring risk, this needs to be mitigated. However, at the same time, the risk management and compliance process cannot be in a bubble, rather they have to work as support for business objectives, which is the moment when governance begins to be relevant as well.

To overcome those obstacles, the complexity of enterprise systems is rising, which creates a demand for one system, which would be able to link them together and allow users or even whole companies to manage them. Therefore, in 2004[2], a company named PricewaterhouseCoopers came up with, at that time, a new term, GRC systems. Although this term is relatively new, there are already many different definitions how to describe these types of systems. One of them describes them as “a management model that promotes criteria unification, as well as communication and collaboration between different stakeholders in management and control of the organization”[3]. While according to a different definition, “GRC is an integrated, holistic approach to organization including wide governance, risk and compliance ensuring that an organization acts ethically and in accordance with risk, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness.”[4]

As already mentioned in one of the definitions, the acronym GRC stands for Governance, Risks and Compliance and each of these terms will be discussed in detail in the next chapter. Even though these topics are nothing new in the IT world and were handled by companies even before the idea of GRC systems, many companies have not approached these activities in a sustainable way and nowadays, they are forced to make enormous investments to handle it correctly and the cost just to handle the compliance process can be up to hundreds of thousands dollars[5]. Due to this fact, GRC systems are interesting especially for large companies with branch offices in multiple countries, where achieving compliance and ensuring legislation is not an easy task. Since it is challenging to implement such a system, there are several companies specialized in GRC systems implementation such as IBM, MetricStream or SAP. A comparison of each solution is done by a company named Forrester on a regular basis and afterwards publicly published as Forrester Wave 0.1.

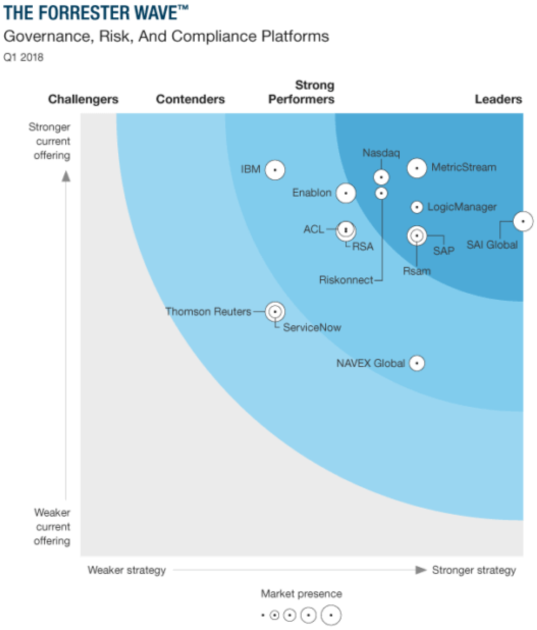


Figure 0.1: Graph comparing several implementations of GRC systems, done by Forrester.[6]

Problem Statements

Companies with a GRC management system are searching for a way how to reduce their operating costs. The model-driven approach for GRC systems has potential to achieve this goal, but whether the complexity of the systems will not be an issue still needs to be investigated.

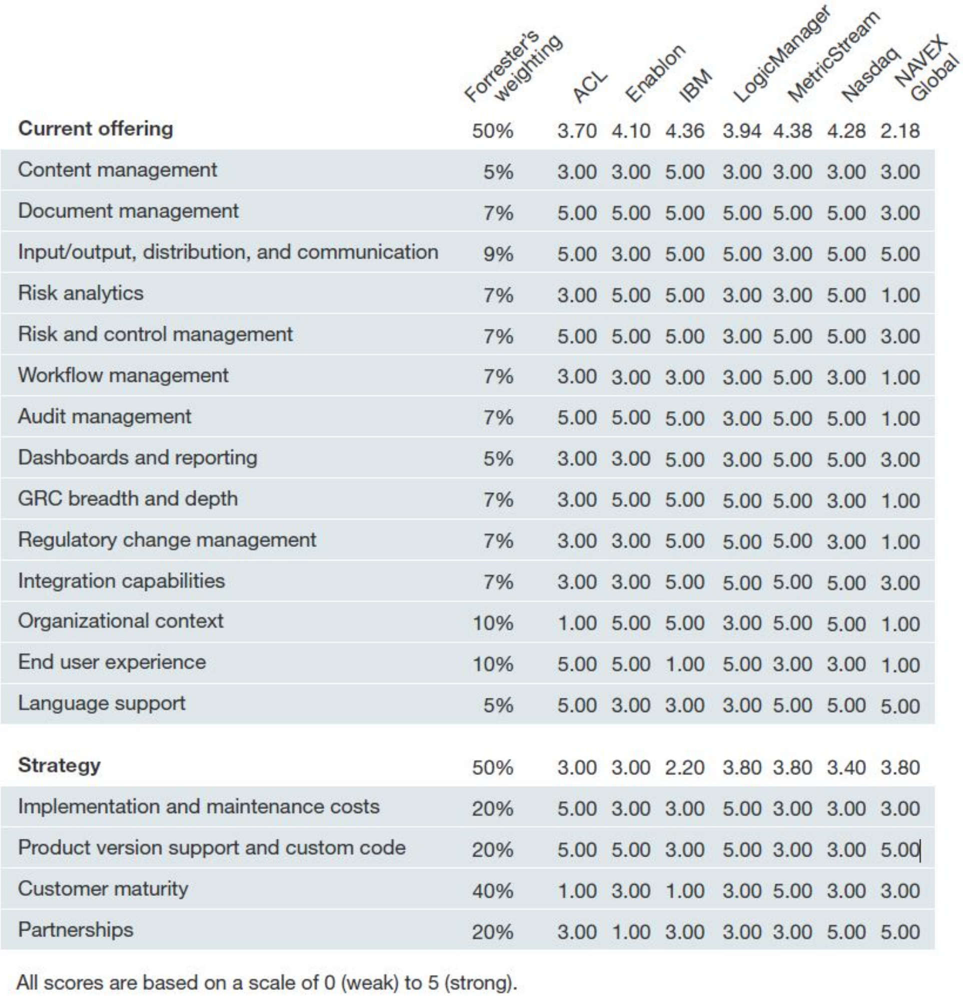
State of the Art

Since the field of GRC systems has huge potential to grow in the following years, there are already several vendors who have developed their own platforms. To demonstrate the growth of GRC systems, Forrester stated in one of their journals[7] that each of the 14 main vendors have already earned more than 30 million dollars in GRC revenue, while having at least 150 clients. Those vendors' platforms differ in many aspects such as content/document management, integration capabilities or organizational context. Since there are so many aspects to be covered by one platform, the approach and way how these systems were developed differ significantly. The Forrester company has divided the main vendors into for categories[6]:

- Leaders
- Strong Performers
- Contenders
- Challengers

Each vendor was categorized based on their results in the sections, current offer and strategy.

As it can be seen from the table 0.2, there are many modules which have to be part of the platform. A simple goal would be to reach the maximum possible score in all areas, but that is quite complicated and therefore even the leaders fail to achieve this. One of the biggest issues is the software architecture of the system, which has to efficiently connect all parts of the system and be opened for future modifications or changes. However, fulfilling those requirements is complicated and also very expensive if the system is not designed correctly. Therefore, a possible implementation of software architecture of a model-driven GRC system will be discussed in the following chapters.



	Forrester's weighting	ACL	Enablon	IBM	LogicManager	MetricStream	Nasdaq	NAVEX Global
Current offering	50%	3.70	4.10	4.36	3.94	4.38	4.28	2.18
Content management	5%	3.00	3.00	5.00	3.00	3.00	3.00	3.00
Document management	7%	5.00	5.00	5.00	5.00	5.00	5.00	3.00
Input/output, distribution, and communication	9%	5.00	3.00	5.00	5.00	3.00	5.00	5.00
Risk analytics	7%	3.00	5.00	5.00	3.00	3.00	5.00	1.00
Risk and control management	7%	5.00	5.00	5.00	3.00	5.00	5.00	3.00
Workflow management	7%	3.00	3.00	3.00	3.00	5.00	3.00	1.00
Audit management	7%	5.00	5.00	5.00	3.00	5.00	5.00	1.00
Dashboards and reporting	5%	3.00	3.00	5.00	3.00	5.00	5.00	3.00
GRC breadth and depth	7%	3.00	5.00	5.00	5.00	5.00	3.00	1.00
Regulatory change management	7%	3.00	3.00	5.00	5.00	5.00	3.00	1.00
Integration capabilities	7%	3.00	3.00	5.00	5.00	5.00	5.00	3.00
Organizational context	10%	1.00	5.00	5.00	3.00	5.00	5.00	1.00
End user experience	10%	5.00	5.00	1.00	5.00	3.00	3.00	1.00
Language support	5%	5.00	3.00	3.00	3.00	5.00	5.00	5.00
Strategy	50%	3.00	3.00	2.20	3.80	3.80	3.40	3.80
Implementation and maintenance costs	20%	5.00	3.00	3.00	5.00	3.00	3.00	3.00
Product version support and custom code	20%	5.00	5.00	3.00	5.00	3.00	3.00	5.00
Customer maturity	40%	1.00	3.00	1.00	3.00	5.00	3.00	3.00
Partnerships	20%	3.00	1.00	3.00	3.00	3.00	5.00	5.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Figure 0.2: Score of GRC Vendors[7]

Chapter 1

Governance, Risk and Compliance

Before getting into the implementation of GRC systems themselves, certain knowledge of parts of the system is necessary in order to fully understand the topic. Therefore, this chapter contains such information and discusses terms connected to GRC in separate sections. Part of the chapter is devoted to the main outcomes of GRC systems.

1.1 Governance

In the past years or even decades, IT governance became a buzzword, which is widely used by many organizations and even receives a lot of attention by the academic world, hence there are countless definitions and is a very broad term. It is not easy to choose the 'right' definition. For the purposes of a GRC system description, the following definition is accurate: "IT governance is the organizational capacity exercised by the board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT."[8]

In other words, governance in terms of information technologies could be defined as a set of simple processes which should ensure effective use of IT in order to support the business goals of a company. Where process could be defined as "a series of actions, changes, or functions that brings about an end or result"[9]. The IT strategy of a company is usually specified by top management, especially by the IT Director (or CIO), who is responsible for cooperation between IT and business units and responds to company's top management. The IT Director defines the organizational structure, defines the resource requirements and often sets how IT governance will be measured and checked.

IT Governance in organization is mainly specified in five different areas[10]:

- **Strategic Alignment**: It is crucial that IT strategy is created based on business strategy, otherwise it is not able to fully support the company's objectives.
- **Value Delivery**: IT should help lower the expenses of the company and by that increase profit and prove the value of information technologies.
- **Risk Management**: Risks should be mitigated in order to prevent IT system failures and ensure the continuity of operations.
- **Resource Management**: Optimizing the usage of available resources (people, applications, infrastructure and information).
- **Performance Measurement**: To ensure requested quality, services and processes are tracked, evaluated and optimized.

Those points induce that there is no question if a company has or does not have IT governance, there is just a question if the governance is handled in the right way. Nowadays, basically all companies are using IT systems to support their business goals, therefore, each of those companies are dealing with an issue how to approach this task. Good governance should create a decision-making framework, which should always provide the company with an answer to the question how the specific process should be handled in order to align with the company strategy.

1.1.1 Standards and Frameworks for IT Governance Support

To assist and support IT governance, there are already numerous standards and frameworks created. In this case, the framework or standard defines the ways and methods for the implementation, management and monitoring of IT governance within the organization. The most well-known are:

- Information Technology Infrastructure Library (ITIL)[11]: A library describing the best practices for delivering IT services. ITIL sets an approach for IT Managers to help companies manage risks and build a stable IT environment. It consists of five core principles: strategy, design, transition, operation and service. Those principles combined provide the basis for a strong IT governance structure.
- The CobiT Framework (Control Objectives for Information and Related Technologies): A good-practice framework developed by ISACA for information technology (IT) management and IT governance. Its purpose is to provide "a set of controls over information technology and organize them around a logical framework of IT-related processes and

enablers."[12] CobiT consists of five components such as framework, process descriptions, control objectives, management guidelines and maturity models.

- ISO 27001[13]: The standard which defines objectives for information security control, which includes IT governance.

1.2 Risk

Since most companies have their data stored online, they became more dependent on information technologies and therefore, their concern about the security of the systems increased. Information is currently one of the most valuable resource of companies, so the ability to keep system secure is creating a business advantage and is an essential success factor. "There are three fundamental qualities of information which are vulnerable to risk and which, therefore, need to be protected at all times, namely availability, integrity and confidentiality."[14] "The risks that threaten the security of its information and computer resources need to be assessed and managed in proper way and the necessary security controls need to be implemented and managed effectively."[15]

The main concern of Information Technology Risk Management is to identify any threats, which could put information systems in danger of a security breach or any unexpected behavior. On top of identifying threats, consequences should be determined and safety mechanisms should be applied in a cost-effective way in order to mitigate (or ideally eliminate) the risk. The International Organization for Standardization defines in ISO 31000[16], risk management should be an integral part of an organization and embedded in the culture of the company. The process of risk management itself is defined in 7 steps:

1. Establishing the Context: The organization sets its objectives and defines parameters, which need to be taken into account when managing the risks and specifies the risk criteria.

2. Risk Identification: The sources of risks need to be identified as well as areas of impact and undesired events, which might occur. The aim is to create a list of risks, which might effect the achievement of the objectives.

3. Risk Analysis: The aim of this step is to get a better understanding of the risk. The output of this point is to get input data for risk evaluation and a decision if the risk will be treated. If so, then possible methods of treatment should be specified.

4. Risk Evaluation: The marked risks, which need to be mitigated/eliminated are compared and priorities are set.

5. Risk Treatment: One of the possible approaches to treating the marked risk is chosen and implemented.

6. Monitoring and Review: This part of the process can be done periodically or happen ad-hoc and should involve surveillance of identified risks.

7. Communication and Consultation: Information about each of the risks being communicated with the stakeholders.

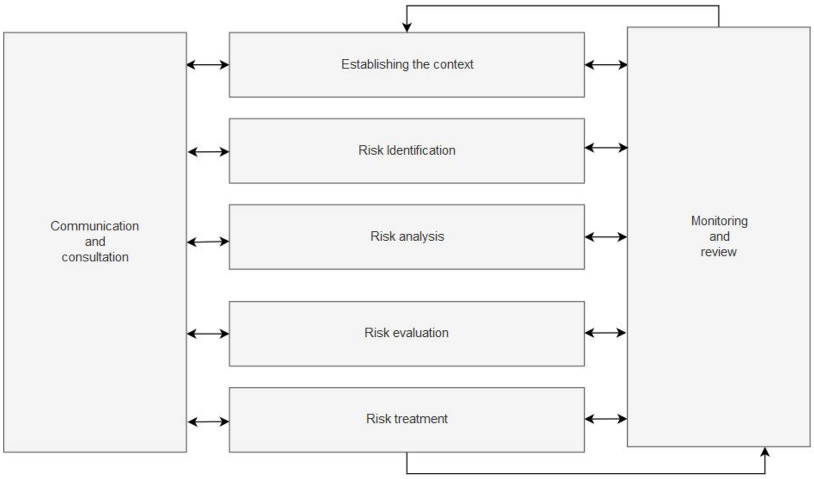


Figure 1.1: The Risk Management Process

1.3 Compliance

To be compliant means to be able to prove fulfillment of a requirement, obligation, commitment, boundary, policy or value and to act with integrity at the same time. The compliance program of the organization involves efforts to comply with local laws (defined by governments) as well as industry or even internal regulations. Being non-compliant can put an organization in danger of being withdrawn or suspended of services, fined or even investigated by federal agencies.

To understand compliance in a little bit more personal way, one can imagine paying taxes, signing a contract with an employer or just being locked out for using an incorrect password. In the context of information technologies, compliance includes activities that maintain and provide systematic proof of both adherence to internal policies and the external laws, guidelines, or regulations imposed upon the company[17]. The role of IT compliance in companies is rising, since the sharing and storing of data has an impact on the several departments such as operations, marketing or legal, depending on the services of IT and their information gathering.

IT compliance can set rules for handling personal data, such as if and for how long specific data can be stored, which security procedures have to be active and if the data can be distributed and to whom. The importance of implementing these mechanisms and rules was increased by the General Data Protection Regulation (GDPR)[18] where companies are facing the risk of getting a fine of 4% of their total worldwide annual turnover.

There are countless international standards as well as state restrictions which make it difficult for companies to identify which regulations they need to be compliant with. There are several international standards which affect IT compliance tremendously[17]:

- Basel III [19]: Regulations which apply to the banking industry and help determine the amount of capital needed for a bank to reserve in order to recover in the case of a loss. This regulation impacts IT, as it needs software that can perform more advanced calculations.

- The Sarbanes-Oxley Act (SOX) of 2002 [20]: Statute to regulate financial transparency and reporting. It was enacted by Congress as a direct response to Enron's and WorldCom's (huge energy and communication providers) misconduct. Section 404 is of significance for IT in the area of financial reporting controls.

- HIPAA [21]: Regulations to which American health care organizations need to comply. It sets rules for storing and transmitting electronic health information.

- PCI DSS [22]: Any merchants accepting credit cards for payment need to comply with this regulation. Rules for the privacy of customer financial data are being set.

1.3.1 Compliance Audits and Reports

"Assessments and audits are a method for determining compliance. Performed by an audit committee, a compliance audit can determine if a company is adhering to the applicable laws by a systematic review of policies, procedures, operations and controls. Since IT has a company-wide reach, an audit is usually done across numerous departments. The scope of an IT compliance audit identifies the laws and requirements, assesses how specific laws, requirements, or standards are being met, and provides recommendations and remedies for non-compliance."[17]

The outcome of the compliance process is IT compliance reports, which are usually required during an audit as proof that the company complies with the regulations. In addition, reports can be used by the IT department as a source of information for uncovering security hazards and potential threats.

1.4 Capability Maturity Model

The Capability Maturity Model (CMM) is a reference model for evaluating companies' processes and to categorize their maturity. This model should help companies move from having ad-hoc or chaotic processes to more organized or mature processes. The CMM itself contains five different levels and each level consists of several areas, which describe specific processes that should be considered by the organization for optimization.

The CMM was originally developed in order to help the American Department of Defense (DoD) choose optimal software suppliers at the end of the 1980s. The suppliers were evaluated on the previously mentioned scale from 1 to 5 and representatives of the DoD used this information as one of the criteria in tenders for new project/software. By doing so, the DoD put pressure on suppliers to improve their processes in order to increase their chance of getting a contract. At the beginning of the 1990s, several multinational companies such as Siemens, Motorola and Schlumberger started to use this model as they recognized the positive outcomes of having their processes aligned with the CMM.[23]

As noted earlier, there are five levels of the CMM:

1. Initial: A very small amount of processes is defined and the rest of the processes are created or done for a particular purpose when it is necessary.

2. Repeatable: Several project management processes are defined in order to track cost or functionality. The basic process discipline is set.

3. Defined: Software processes for project management and engineering activities are defined and documented. They are used in organization to standardize the flow of software development projects.

4. Managed: The software development process and quality management are defined and measured in detail. Processes and products are regularly controlled.

5. Optimizing: Thanks to the usage of quantitative feedback from processes, continuous process improvement is in place for innovative ideas and technologies.

"The CMM is a descriptive model in the sense that it describes essential (or key) attributes that would be expected to characterize an organization at a particular maturity level. It is a normative model since the detailed

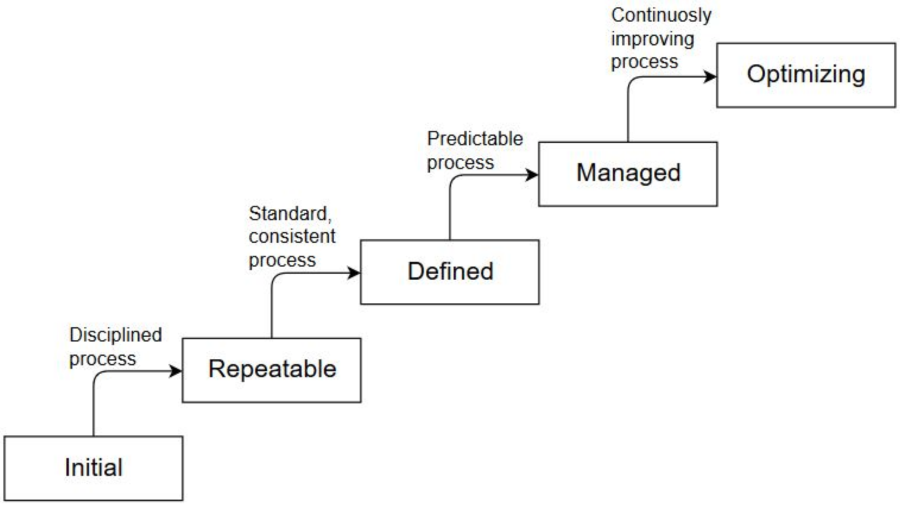


Figure 1.2: The Five Levels of the Capability Maturity Model[24]

practices characterize the normal types of behavior that would be expected in an organization doing large-scale projects in a government contracting context. The intent is that the CMM is at a sufficient level of abstraction that it does not unduly constrain how the software process is implemented by an organization; it simply describes what the essential attributes of a software process would normally be expected to be."[24]

The CMM does not set a way how the processes should be improved, therefore, it can not be used as a manual, to get to a higher level maturity model. It simply describes reference or model organization at each of its maturity levels. To move from a level to the next one can take a few years.

1.4.1 GRC Capability Model

Although the CMM is focused on IT governance, the GRC Capability Model goes a little bit further. Since a concern of the GRC system is also about compliance and risks in this case, the CMM is extended by additional components in order to fully support universal and organization objectives. As displayed in figure 1.3, the GRC Capability Model consists of 4 integrated components[25]:

- Learn: Examine and analyze context, culture and stakeholders to learn what the organization needs to know to establish and support objectives and strategies.

- Align: Align performance, risk and compliance objectives, strategies, decision-making criteria, actions and controls with context, culture and stakeholder requirements.

- Perform: Address threats, opportunities and requirements by encouraging desired conduct and events, and preventing what is undesired, through the application of proactive, detective and responsive actions and controls.

- Review: Conduct activities to monitor and improve design and operating effectiveness of all actions and controls, including their continued alignment to objectives and strategies.

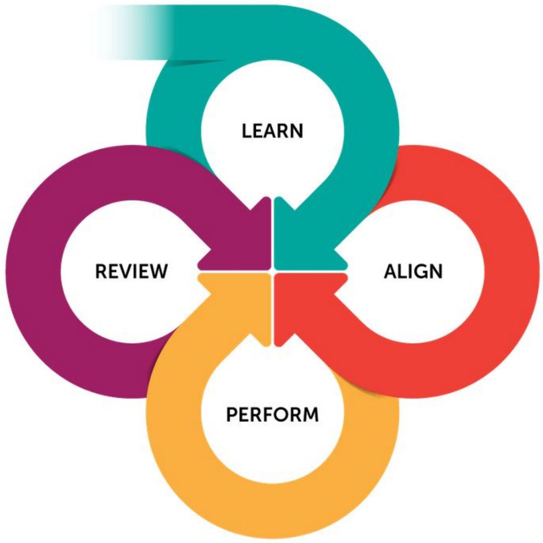


Figure 1.3: The GRC Capability Model[25]

1.4.1.1 Principled Performance

Principled Performance is a term which is quite often connected with the GRC. In this case, it is a vision or approach how to reliably achieve objectives while addressing uncertainty and acting with integrity. This means that in order to succeed, an organization needs to find a way how to deal with unknown factors and unexpected circumstances. Anything uncovered has to be well-documented in order to be trustworthy. For any new discoveries, an organization must find a way how to consistently evaluate them and treat them. Again, any of these evaluations need to be documented.

The outcomes of principled performance can be defined through high-performing, GRC capabilities. The goal of every organization should be to achieve these universal outcomes:

1. Achieve business objectives: The whole organization has to work together towards the achievement of enterprise objectives.

2. Ensure risk awareness settings for objectives and strategic planning: Risks and responsibilities need to be regularly reported to relevant stakeholders.

3. Enhance organizational culture: Build and promote a culture of performance and integrity.

4. Raise stakeholder confidence: Increase the trustworthiness of the organization.

5. Prepare and protect the organization: The organization has to be prepared to address risks and be protected from any possible difficulties.

6. Prevent, detect and reduce adversity and weaknesses: Control mechanisms have to be set in order to address issues as they arise.

7. Motivate and inspire desired conduct: Desirable conduct has to be rewarded.

8. Stay ahead of the game: In order to support changes in the strategy of the organization, new information imports for that purpose, need to be learnt fast and efficiently.

9. Improve responsiveness and efficiency: Capabilities should be defined in order to be more responsive end efficient.

10. Optimize economic return and values: Human and financial resources should be allocated in a way to optimize economic return while maximizing its values.

Chapter 2

GRC Systems

GRC systems integrate disciplines of governance, risk and compliance into a single platform. Such integration helps optimize inner processes, since it is possible to create and coordinate policies which can enforce the fulfillment of compliance requirements.

2.1 Goals of GRC Systems

There are many benefits of GRC systems and several of them are already described by the definition, but there are just a few of them, which all companies should seek to accomplish[26]:

- **To achieve business objectives**: The main objective of GRC systems should be to support the business goals of the organization.
- **To ensure risk aware setting of objectives and strategic planning**: The system should be able to provide regular, reliable information about risks to certain authorities and managers responsible for execution.
- **To increase stakeholder confidence**: Through the transparency of the organization, raise stakeholder trust in the company.
- **To prepare and protect the organization**: Prepare the organization to address risks and requirements while protecting the organization from adversity and surprises and enabling it to grasp opportunities.
- **To prevent, detect, and reduce adversity and weaknesses**: Certain actions need to be established in order to prevent negative outcomes, minimize impact and detect potential problems.
- **To stay ahead of the competition**: Information needed to support strategic and tactical changes or to avoid obstacles and pitfalls should be received by managers as soon as possible.

- **To optimize economic return and values**: The system should support a company, so it is possible to allocate human or financial resources in a way that maximizes the economic return generated for the organization while maximizing its values (could be, for example, the outcome of an internal audit).

Several additional goals could be of course found to support the idea of GRC systems, but in the end, it will always be related to the support of business objectives. Even though that is probably the goal of all information systems, GRC systems differ in this way (as it will be discussed further) and should work like an umbrella covering all internal (and even in some cases external) systems. There might be some of the opinion that Enterprise Resource Management systems (ERM) are basically the same, but that is not exactly true. ERM systems are missing the compliance aspect, they are mitigating risks, but without context knowledge since they are not fully covering governance. Due to that, it can be expected that demand for GRC systems will rise.

2.2 Components of GRC Systems

Systems contain many different modules in order to manage risks, contents, documents, accesses and many other parts of IT systems. Differences can be seen even among main vendors, where some components of theses systems are less developed or not developed at all. However, the core of the system stays mostly the same, therefore, only the main components will be mentioned in the following list.

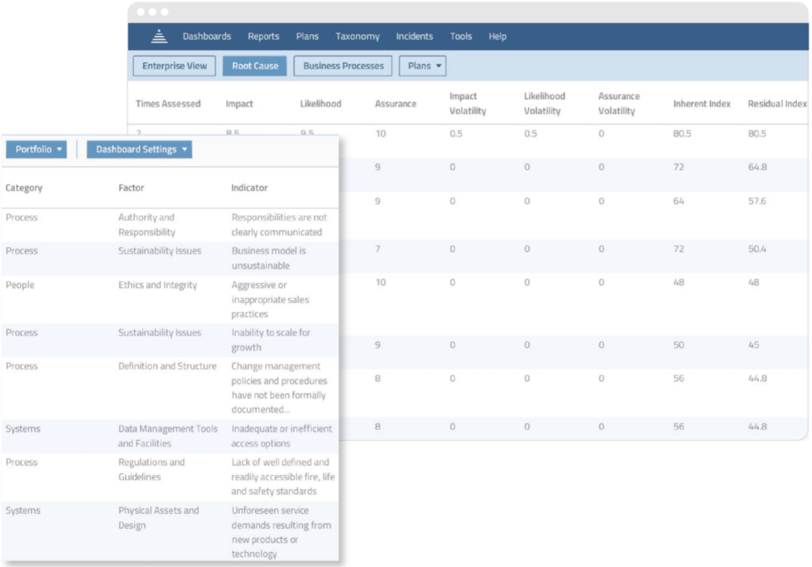
There are several major components:

- Workflow Management: This component handles the workflow of the applications or systems inside the company. It allows users to define sequences of tasks, automatic routing or notifications.

- Risk and Control Management: This component is used to address risks and manage or mitigate them. It deals with the whole risk process from risk identification through risk assessment/evaluation to risk monitoring.

- Audit Management: The goal of this part of the system is to simplify and organize the work flow and collaboration process of compiling audits. Since shared folders or emails are still widely used by many audit teams, this can help share the results of audits and make cooperation among teams more efficient.

- Content Management: This component supports the collection, management and publishing of information in any form. Information is addressed as content which can be any document, audio or video file and many others.



Times Assessed	Impact	Likelihood	Assurance	Impact Volatility	Likelihood Volatility	Assurance Volatility	Inherent Index	Residual Index
2	8.5	9.5	10	0.5	0.5	0	80.5	80.5
			9	0	0	0	72	64.8
			9	0	0	0	64	57.6
			7	0	0	0	72	50.4
			10	0	0	0	48	48
			9	0	0	0	50	45
			8	0	0	0	56	44.8
			8	0	0	0	56	44.8

Category	Factor	Indicator
Process	Authority and Responsibility	Responsibilities are not clearly communicated
Process	Sustainability Issues	Business model is unsustainable
People	Ethics and Integrity	Aggressive or inappropriate sales practices
Process	Sustainability Issues	Inability to scale for growth
Process	Definition and Structure	Change management policies and procedures have not been formally documented...
Systems	Data Management Tools and Facilities	Inadequate or inefficient access options
Process	Regulations and Guidelines	Lack of well defined and readily accessible fire, life and safety standards
Systems	Physical Assets and Design	Unforeseen service demands resulting from new products or technology

Figure 2.1: The Risk Management Module[27]

- Document Management: This component tracks, manages and stores documents.

2.3 GRC Vendors

To demonstrate the complexity of the systems, three platforms will be briefly discussed. For these purposes two leaders in the market (MetricStream and LogicManager) were chosen as well as one strong performer in this field (IBM). Discussion shows that even large technological companies are struggling with the development of a perfect system.

2.3.1 MetricStream

One of the biggest vendors which has successfully delivered their product, the MetricStream M7 GRC platform, to clients across several industries including insurance, energy, health care and automotive has recently focused on the innovation of their user interface design. The creation of a unique user interface slowed down other development and suddenly MetricStream has to invest in analytic tools to keep pace with the other vendors.

2.3.2 LogicManager

LogicManager took a slightly different path than its competitor MetricStream and put pressure on its customer support. Each client has two analyst advisors at their disposal with no additional costs. Customer support in combination with very fast deployment of their solution help the company get several new, big clients.

2.3.3 IBM

IBM and their IBM OpenPages GRC platform is known for their developed analytic and reporting tools and especially their financial control management and strong operational risk platform is popular among clients. However, its user interface and overall strategy of customer maturity requires huge improvement.

2.4 Case Studies

Since the GRC system is a very sensitive topic for most companies, usually any related documentation is classified. Due to this fact, it was not possible to publish or even find a use-case with detailed information. Even though every company keeps their information about using the GRC system a secret, one of the biggest vendors of this solution, MetricStream, publishes anonymous use-cases on their websites.

2.4.1 Bank

The subject of this use-case study[28] is a large multinational bank with branches in many countries. Through the years, it became an issue to identify which branch should undergo the audit. Audits themselves were complicated, since tools used to conduct them were spreadsheets. Reporting results were also done in a spreadsheet and therefore, the evaluation of the results and decision-making, which should be supported by the outcomes of audits, were complicated and time consuming. Other reasons which upped the pressure to improve internal processes were the increasing requirements for compliance, due to the reform of Basel II, SOX and other regulations.

After discovering all of the requirements, one of the vendors of GRC systems came up with a solution in form of an Audit Management System. It streamlined and automated the process of conducting audits. As a result, auditors can now focus more on critical analysis than on entering the data into spreadsheets. The system performs a risk assessment for each branch based on several factors such as outstanding regulatory or internal issues and can recommend branches, where an audit should take place. All of the results are stored in one place and due to this fact, the system is able to generate reports of the overall results. Reports contain filtering options and any two branches can be compared or even the progress of a branch can be compared to a series of pre-set milestones. Reports are always at disposal for management.

2.4.1.1 Outcomes

- Unification of process for multiple global audits: The system is used by more than 300 auditors worldwide. It provides features such as plan, manage and track audits.

- Increased efficiency: Data moved from spreadsheets into the system, which generates reports and provides management with information about which branch should be audited.

- Minimized recurrence of audit issues: Every issue which arises during the auditing process is investigated and analyzed. Automated notifications and escalations help solve issues effectively and decrease the possibility that the issue will occur again.

2.4.2 Chemical Manufacture

A multi-billion dollar Indian company[29] working in the chemical industry had faced an issue of enormous expenses for compliance. Since the company was operating worldwide and was divided into several business units, each of the business units had to fulfill many different requirements and comply with many restrictions. The HR department and taxation department had their own set of rules which had to be followed. Since the company is working in the chemical industry, the supply chain management had to deal with rules for handling hazardous and non-hazardous materials. Generally speaking, even each factory had to follow some specific rules according to its location, such as effluent waste treatment, union laws, trading-related reports or filling rent renewals.

It was a nearly impossible task for the central compliance team to meet all of the requirements defined by local authorities. To make it even more complicated, each business unit within the company had their own processes and systems. Each quarter of the year, there were approximately 20,000 tests performed, where some of the tests were documented in spreadsheets, while the others in systems. That had to be changed, since there was pressure from the company's managers to create centralized systems, which would manage all of the tests and would be able to create aggregated reports in reasonable time. On top of that, some of the business units had issues performing tests and filing the data on time, therefore, there were email notifications, which were dispatched manually by the central compliance team.

For the above reasons, the company had used the services of one of the GRC vendors in order to improve their IT infrastructure. The vendor designed a system, which was later implemented. This web-based solution allowed the company to manage and monitor all of their manufactures and business units, mapped all their compliance processes and unified reporting. This integrated data model approach has made it possible to track the status of compliance at various levels. Each business unit had access to the system, so it was possible to move all of their compliance tests there and stop using spreadsheets. Part of the solution was automated emails with alerts or notifications which helped pass all of the tests on time without any delays.

2.4.2.1 Outcomes

- Efficient compliance processes: Instead of using their own system, each of the business units used the centralized solution to perform compliance tests and report results.
- Centrally defined processes: All of the processes are mapped in the system. Therefore, any manager interested in a specific branch or business unit can easily access and view the status of its compliance processes.
- Consistent compliance reporting: All of the performed tests are reported and accessible from the system.
- Automatization of processes: The central compliance team does not have to dispatch email notifications anymore since everything is monitored and done by the GRC system.

2.4.3 Media Corporation

This client[30] was one of the leading conglomerates in the field of entertainment and media with over 20,000 factories all over the world. With this number of factories and enormous amount of workers it was very expensive to keep track of all social compliance audits which took place (approximately 15,000 audits per year). The fact that the factories were located in different countries prevented the possibility of having one prefabricated audit since the policies of each of the countries had to be considered. An audit was based on multiple parameters such as child labor, working hours, benefits, labor safety and many others.

Over the years, the client's own compliance management system could not keep pace with every newly opened factory as information required for the audit had to be extended. On top of that, the former solution did not have any dynamic reporting tool, so creating reports got old in a matter of months. Due to these facts, the decision to implement a GRC system was made. One of the requirements was to integrate all of the data, facilitate future audits and create an automatic reporting system. Another key concern was the availability of the data. There was no mechanism how to deliver the audit data to the headquarters, so people in management did not have access to the immediate results. Due to their experience in social compliance solutions, a certain company was selected as a vendor for the solution.

The supplier of the system implemented a cloud-based solution, which integrated all of the gathered data of social compliance audits for almost two decades. Since the client has factories in many countries and is still growing, the implemented solution had to be flexible enough to integrate newly opened affiliated companies and add new types of data, which would be required for audits by local law entities.

2.4.3.1 Outcomes

- Classification of factories: Each factory is categorized according to several parameters such as location, previous audit data or geo-political situation. According to that, a decision on how often it is necessary to conduct an audit is made.
- Data in one place: The implemented solution maintains factory data, results of previous audits, contract details or even a connection to other factories.
- Audit management: The system allows scheduling an audit and creates and assigns audit tasks to relevant people. Audit data is tracked, including auditors profiles, results and violations.
- Centralized reporting: One of the burdens of the former system was outdated reports. The current solution supports automatically generated reports containing all relevant information with trend graphs comparing the results of the audit with previous ones.
- Multi-language support: Since the client is operating in many countries, a language barrier is present basically on a daily basis. Therefore, a solution was implemented that automatically dispatched emails containing information about assignments and corrective actions automatically translated into the user's preferred language.

Thanks to the GRC system, the company was able to reduce the cost of audits. The process became more efficient since the audit workflow was unified. Nowadays, the company's management has fast access to data and can make decisions based on aggregated results.

2.5 BPM Systems

BPM systems are in several ways similar to GRC systems, therefore, it is also important to mention them before comparing them to GRC systems. Since BPM is a widely used term, there are already many different definitions. However, this thesis will be working with the following definition: "Business Process Management (BPM) is a discipline involving any combination of modeling, automation, execution, control, measurement and optimization of business activity flows, in support of enterprise goals, spanning systems, employees, customers and partners within and beyond the enterprise boundaries."[31] In other words, BPM systems, like GRC systems, are optimizing the processes and their goal is to support enterprise goals. However, BPM is more focused on the governance, therefore there is usually a present environment to identify and capture those processes and visualize them by BPMN 2.5.2. The captured processes can be later executed by humans, systems or by a combination of both. By monitoring those processes, companies can obtain information about which process should be improved. The reason for improvement is normally to lower expenses and increase efficiency. This whole process is called the BPM lifecycle 2.2.

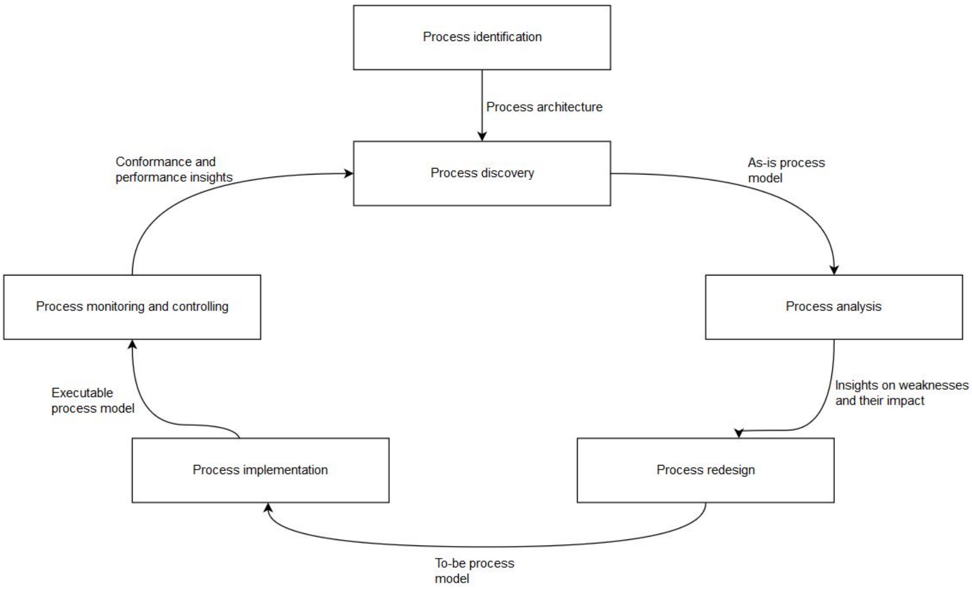


Figure 2.2: The BPM Lifecycle[32]

2.5.1 BPM Vendors

Similar to the GRC market situation, there are many vendors selling various solutions for BPM systems. The table with the vendors and their comparison is provided by Forrester, who publishes a report called Forrester Wave: BPM Platforms for Digital Business. In this report, there are stated market leaders and strong performers such as PegaSystems or IBM as well as contenders and challengers such as Red Hat 2.3.

2.5.1.1 PegaSystems

In order to mention one vendor a little bit more in detail, a solution from PegaSystems was chosen[33]. This company has a long history of software development especially CRM applications that offer various functionality for the user. It starts with sales and marketing activities and continuous with customer service. The system contains a low-code platform to simplify the modelling and creation process.

The Pegasystems platform consist of several environments such as content or case management, application integration, process flow definition, entire mobile application development solutions and many other functions in one model-based development and run-time architecture. On top of that, the platform also contains a low-code platform to simplify the modelling and creation process.

2.5.1.2 IBM

Another major player in the field of BPM platforms is IBM[34]. The same as PegaSystems, IBM has a long history of software development. Their products are used by many companies and contain many features to design, execute and monitor processes.

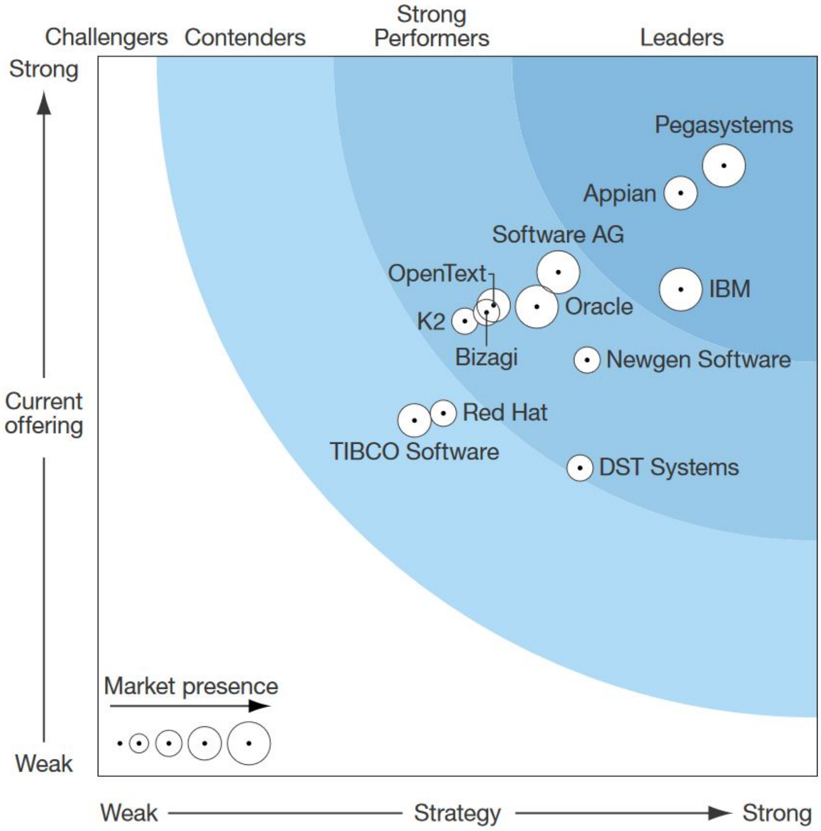


Figure 2.3: Forrester Wave: BPM Platforms for Digital Business[35]

2.5.2 BPMN

Business process management notation is a graphical representation to capture processes and display relations among them. This language consists of more than 100 symbols, which makes it fairly complex. The symbols are used to display the start of the process, processes, transactions, data objects, messages and many others.

2.6 Low-code Platforms

A low-code development platform (LCDP) is software enabling the creation of applications through a graphical user interface. Therefore, users of the platform do not have to know any traditional programming language in order to create the application. However, products of the platform are limited to the possibilities of the platform itself and usually customization is expensive to develop. LCDPs usually focus on a particular kind of application such as web applications, databases, business processes and many others.

As discussed in the article[36] published by Forrester, there are a few major reasons to use low-code platforms:

- Faster implementation and delivery: Parts of the system can be premade modules, which can be connected and deployed via graphical user interface.
- Suitable even for large-scale applications: The product of the platform can be used across the enterprise or by multiple departments.

In the field of low-code platforms there are several top companies, which are the leaders in this market, such as Appian (3.4), OutSystems or Mendix.

2.7 Custom Development

The product of custom development is custom software, which is specially developed for some specific reason. It can be fully adjusted to the needs of an organization for which it is being implemented. It can be considered that on the opposite side of custom software is existing free software or software packages created for the mass market.

Since it is usually implemented for one organization and one project, custom software should completely fulfill organization requirements. The downside of custom development is the price to create such software. Since everything is usually implemented from scratch, it requires many resources to deliver such a product. Development would follow the standard way of software development, therefore, at the beginning there should be a part, where business requirements are gathered, analyzed and based on the outcome of

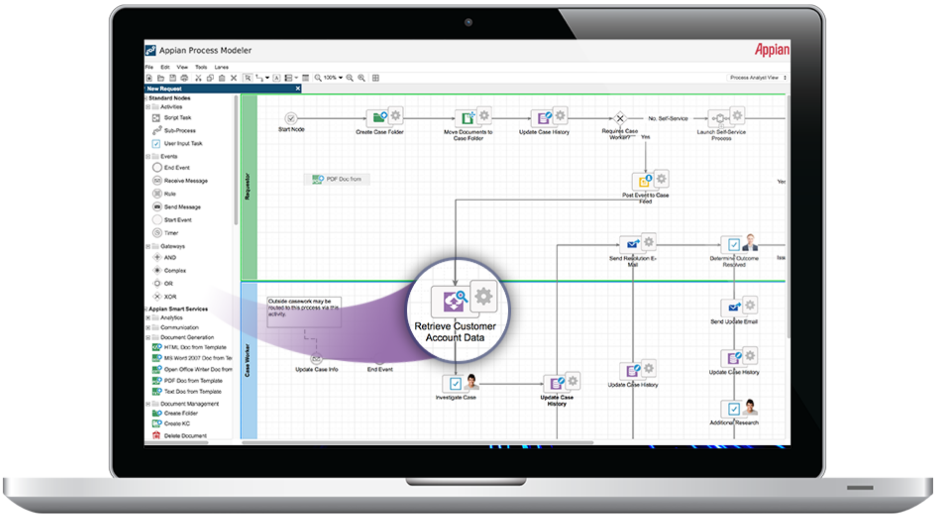


Figure 2.4: GUI of the Appian Process Modeler[37]

analysis, then the product is designed. Another stage would be programming and testing the application, which precedes delivery.

Chapter 3

Comparison of Systems

This chapter is devoted to conduct a comparison of systems defined above (i.e. GRC and BPM systems and low-code platforms). Each of these systems will be given a score according to the number of areas they cover. Since the borders between the systems are blurry, a comparison is not that simple. A BPM system can implement a GRC system, a low-code platform can create a BPM or GRC system and custom development basically covers all systems mentioned in this chapter (which is the reason why custom development was excluded from the comparison). However, each of these systems has its advantages and disadvantages, which will be the object of discussion.

3.1 Comparison Criteria

As mentioned, each system will be given a score according to the areas they cover. The following areas will be ranked:

- Process design tools 3.1: To create and define processes, we often need an environment, which would allow us to do design processes. The easiest way to create this environment would be to write specifications in a simple text editor and deploy those specifications to some process engine. However, this solution requires knowledge of some specific language, which would be used to model such processes and that could be a dead end for many users. Therefore, the system should contain a drag-and-drop graphical user interface, where the user can simply choose the elements they want to use and by that create and visualize those processes. This way is more accessible for the common user and therefore, a platform with such an environment has a bigger chance of success in the market when compared to other platforms.
- Process automation: On top of creating the processes, systems should allow the user to deploy the process flow to the server, where it would be automatically executed in defined intervals.

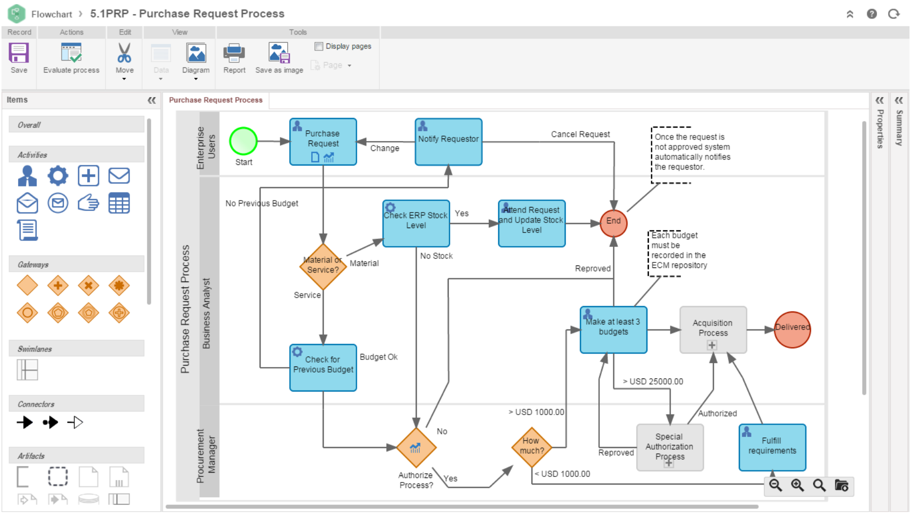


Figure 3.1: Business Process Modelling[38]

- Activity monitoring: The system should allow users to access information regarding its activity and history 3.2. The goal is to have the ease to follow dashboards with relevant information about the status of the system.

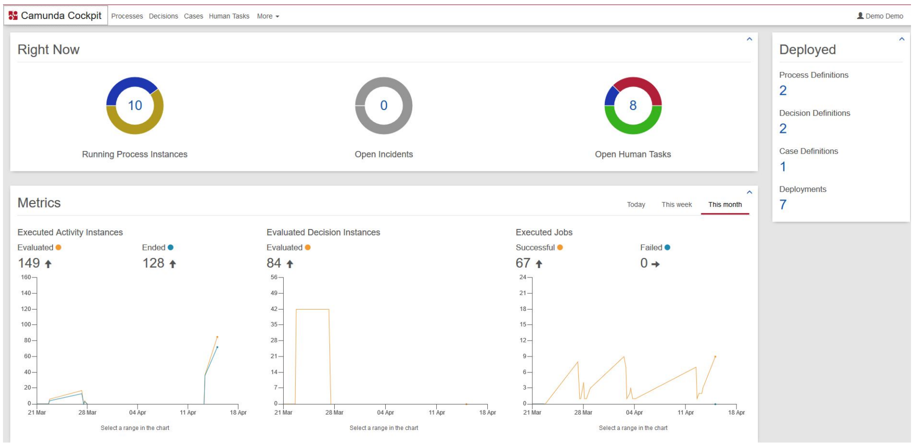


Figure 3.2: Activity Monitoring: The Camunda Cockpit[39]

- Automatic reporting: This area includes several functions which are above standard activity monitoring, such as regular, automatic creation of reports, automatic mailing based on specific events or a comparison of information over time. This kind of report can happen automatically (i.e. at the beginning of every month) or can be triggered by the occurrence of an incident.

- Suitable to mobile devices: The systems should be accessible from mobile devices. Each user with access to the system should be allowed to check the system (especially if activity monitoring is present) from their smartphone with the screen correctly adjusted to the screen size.

- Integration with client's systems: The system should allow easy integration with other systems such as CRM or databases.

- Document management system 3.3: Since documents (and digital content in general) is quite often part of business processes, the system should allow their management, which includes features such as version control, document generation, easy search and retrieval.

- User management: Since business processes usually cover many different topics, users should be allowed to access only several specific processes (and their content). Therefore, the system should be built in a way that makes user hierarchy and different access rights possible.

- Vendor risk management: Sometimes it is necessary to use third-party software and implement it in one's own infrastructure. Nonetheless, it should always be considered a risky action. Therefore, each possible vendor should be evaluated and selected based on the level of potential risk.

- Risk analytics: Before managing risks, it's necessary to discover them and analyze them. Systems should provide a tool to users that simplifies their analysis of a risk.

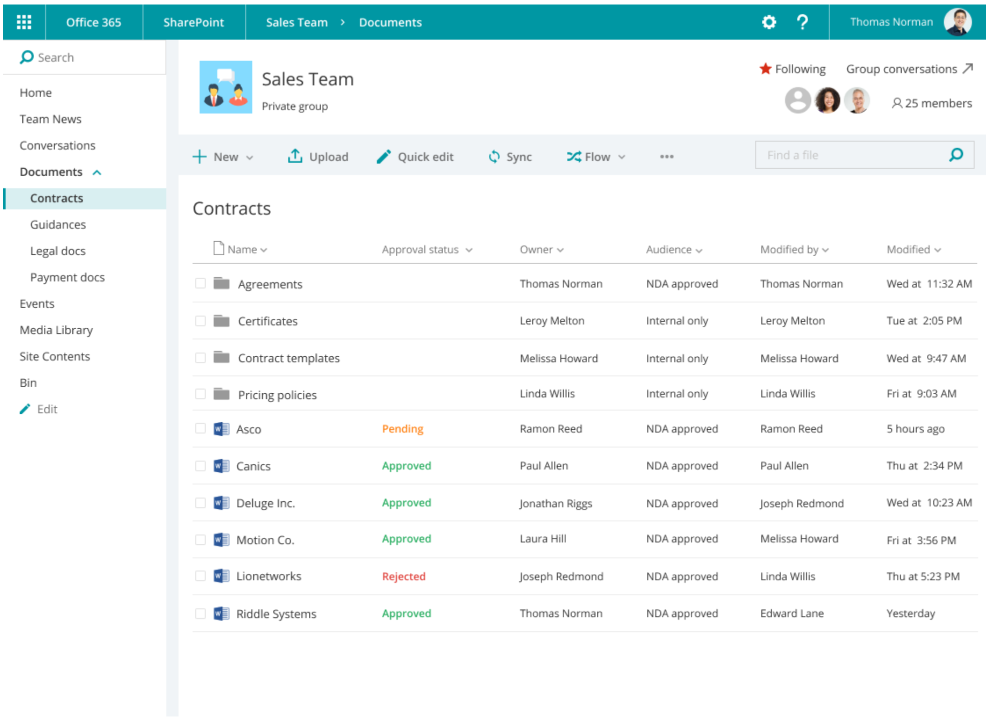
- Risk management: Each process should be possible to evaluate by the risk involved. The environment should allow the user to go through the whole risk process, from risk identification through to risk evaluation.

- Risk monitoring: Each risk defined by risk management has to be monitored, so relevant users are notified about potential threats.

- Policy management: The functionality to define rules or policies for specific situations. To some extent this component works like an alert system. If an event defined by policy management occurs, it can trigger notifications to the system administrator to mitigate potential threats.

- Compliance management: The environment that handles all compliance requirements, such as regulatory risks or rule mapping. Activities also include managing audits. Audits should be able to track and report accordingly.

- Audit management: Support of internal audits. Since audits are often conducted on a regular basis, organizations should have the possibility to manage those audits effectively.



Contracts

Name	Approval status	Owner	Audience	Modified by	Modified
Agreements		Thomas Norman	NDA approved	Thomas Norman	Wed at 11:32 AM
Certificates		Leroy Melton	Internal only	Leroy Melton	Tue at 2:05 PM
Contract templates		Melissa Howard	Internal only	Melissa Howard	Wed at 9:47 AM
Pricing policies		Linda Willis	Internal only	Linda Willis	Fri at 9:03 AM
Asco	Pending	Ramon Reed	NDA approved	Ramon Reed	5 hours ago
Canics	Approved	Paul Allen	NDA approved	Paul Allen	Thu at 2:34 PM
Deluge Inc.	Approved	Jonathan Riggs	NDA approved	Joseph Redmond	Wed at 10:23 AM
Motion Co.	Approved	Laura Hill	NDA approved	Melissa Howard	Fri at 3:56 PM
Lionetworks	Rejected	Joseph Redmond	NDA approved	Linda Willis	Thu at 5:23 PM
Riddle Systems	Approved	Thomas Norman	NDA approved	Edward Lane	Yesterday

Figure 3.3: Microsoft Sharepoint[40]

3.2 Summary

Each of the system was evaluated based on how developed these components or modules are. The complexity and flexibility of the solution were also taken into consideration. The following scale was used for the evaluation:

- Fully covered: The system fully supports this feature and is present in most delivered solutions.
- Partially covered: The component is present in the system, however, it does not contain complex functions or is not usually used.
- Not covered: The component is not present at all or requires enormous resources to adapt it to clients needs.

Each of these systems are suitable for different purposes. At first glance, one might expect that since GRC almost fully covers BPM that there would be no competition between those two systems. However, since BPM focuses so much on processes, its design tools and long development history make it a reasonable choice for companies, which do not have to worry about compliance much.

	GRC Systems	BPM Systems	Low-code Platforms
Process design tools	PC	FC	FC
Process automation	FC	FC	PC
Activity monitoring	PC	FC	PC
Automatic reporting	FC	PC	NC
Suitable for mobile devices	NC	PC	NC
Integration with client's system	PC	PC	PC
Document management system	FC	FC	FC
User management	FC	FC	FC
Vendor risk management	PC	PC	NC
Risk analytics	PC	PC	PC
Risk management	FC	PC	PC
Risk monitoring	FC	PC	PC
IT policy management	PC	PC	NC
Compliance management	FC	NC	NC
Audit management	FC	NC	NC

Figure 3.4: Comparison of Different Systems on FC (fully covered), PC (partially covered) and NC (not covered) Scales.

Chapter **4**

Software Architecture of GRC Systems

For the purposes of this chapter, a use-case from the real world will be considered when designing the software architecture of the GRC system. Since GRC systems are quite often used in the banking sector, the proposed architecture will be created for a bank. This type of institution is suitable for this case study for several other reasons. There are strong compliance requirements and since banks are quite often operating in several different countries, government regulations differ and to conduct an audit (and be able to report results) requires complex software such as a GRC system.

Due to the fact that designing an entire GRC system is a task for a whole team of analysts, the use-case is simplified and the architecture will be designed for a virtual bank (or as sometimes referred, a direct bank). This means that all services are facilitated by an information system without any software engineers or any other employees. There are no branches and everything is done online. Thanks to its infrastructure, these banks can offer higher interest rates.

Even though a virtual bank is being considered, compliance requirements need to be handled, especially if the bank would be running in multiple countries. Therefore, there is one Central Virtual Bank, which has a link to local virtual banks as displayed in the figure 4.1.

4.1 Conceptual Model

Given the conditions defined in the previous sections, the architecture of a virtual bank 4.2 can be created accordingly. The designed architecture consist of four main parts:

1. User Interface: Any connection between the user and the bank is considered as user interface. The bank can be accessed through channels

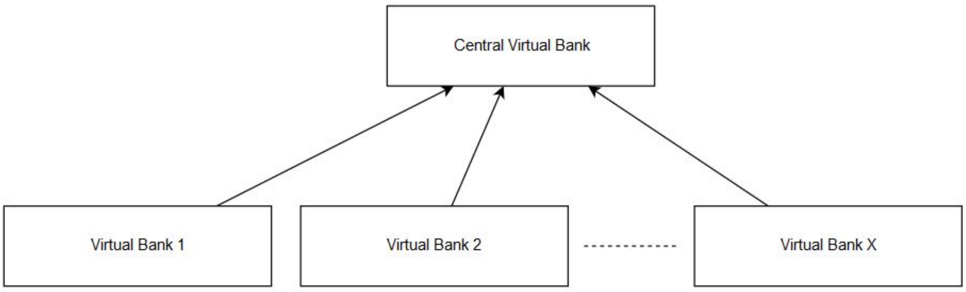


Figure 4.1: Organizational Structure of a Virtual Bank

such as the Internet or mobile devices. The reason why any contact is done via user interface is due to the fact that we are considering a purely virtual bank, therefore, there are no branches nor ATMs.

2. Services: On this level we distinguish between sales/service and customer relationship management. In the sales/service part, retail, corporate, private and commercial banking is covered.

3. Operations: The third level of architecture covers operations such as payments, reporting systems, bank treasury or even IT development.

4. Analysis Systems: Each bank has its own supervision activities to ensure that the bank complies with the regulations and restrictions, to perform audits or detect frauds.

In order to fulfill compliance requirements it is necessary to create a model which can be connected to related frameworks such as Basel. Therefore, the proposed architecture was designed with regard to this requirement.

The architecture in the figure 4.2 has been designed for a virtual bank. If we would be designing an architecture for a central virtual bank, the schema would be slightly different. Since a central virtual bank fulfills supervisory role in this model, there would be no user interface and no services for customers. There would just two levels:

1. Operations: Part of the system handling reporting, payments or regulations.

2. National Supervisory System: It is a GRC system itself with all main parts (Governance, Risks and Compliance), therefore, all key information is gathered here, analyzed and classified.

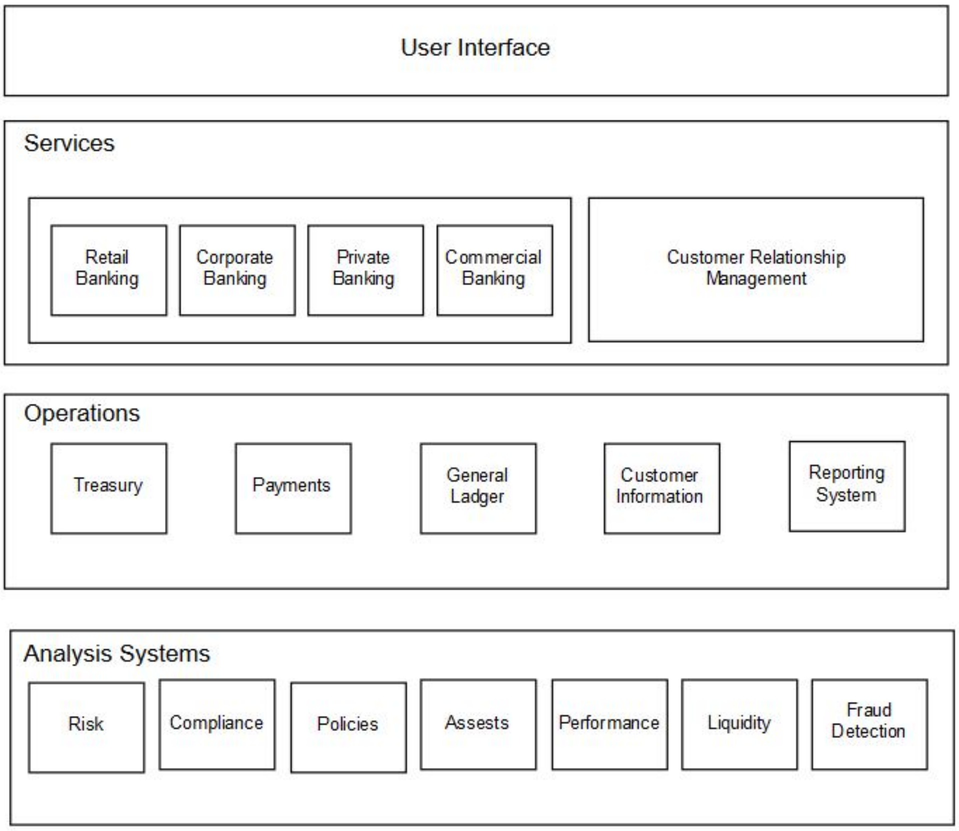


Figure 4.2: Architecture of a Virtual Bank[41]

4.2 Use-case Model

Since the role of a central virtual bank and virtual bank differs, the use-case diagram will be modelled for both roles. It captures information how the entity interacts with the system and what possible actions are.

4.2.1 Virtual Bank

The use-case model for this role 4.3 is created based on its architecture 4.2. Either the organization or private clients are customers in this use-case, who can access bank accounts and operate with their funds. A more complex role in this case is the system (Virtual Bank) itself. On top of handling customers, it also accesses several other components of the system, which are analyses and reports. It is not just risk and compliance which are being reported, it can also include customer satisfaction measured through the customer relationship management.

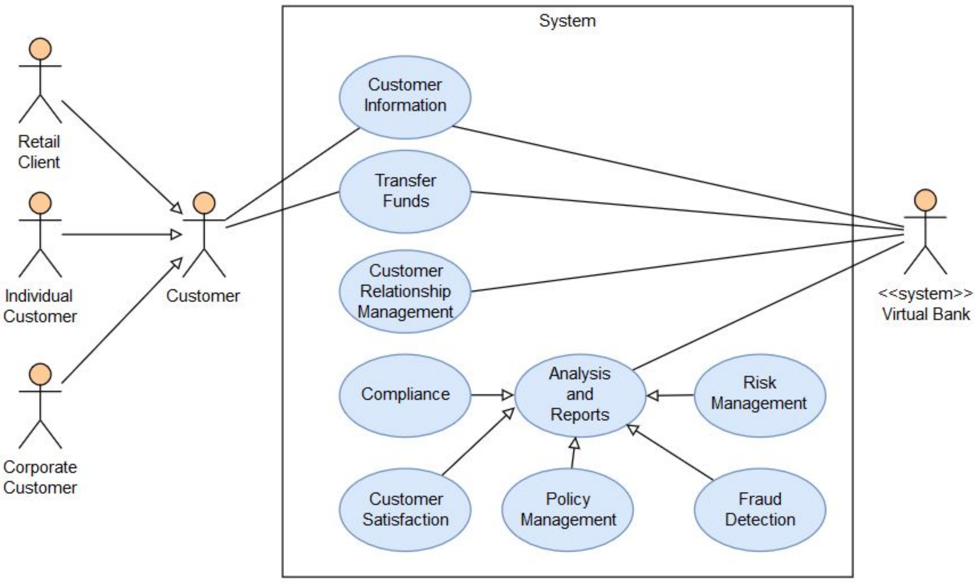


Figure 4.3: Use-case Model of a Virtual Bank

In our case, the diagram consists of the following use-cases:

- Customer Information: Storage of customers' personal information.
- Transfer Funds: All of the operations which can be done by customers like payments, investments or loans.
- Customer Relationship Management: The part of the system managing all of the company's relationships and interactions with customers.
- Analysis and Reports: A huge use-case which covers all of the analyses and reports created within the system.
- Compliance: Compliance reports are generated here. This component is under control if all of the actions comply with the regulations. These regulations are usually defined at the level of a central virtual bank.
- Customer Satisfaction: Via customer feedback, the organization can take steps to improve their processes in order to keep current customers and even get new ones.
- Policy Management: This component compares the current situation with internal policies and creates a report accordingly.
- Fraud Detection: An analytical part of the system, which goes through the data stored in the system and reports any deviation from the standards.

- Risk Management: Another analytical part of the system controlling all of the risks.

4.2.2 Central Virtual Bank

A GRC system which is present in a central virtual bank extracts information from all virtual banks, classifies them into governance, risks and compliance and defined actions take place. For example, alerts or additional reports are being generated and dispatched 4.4. Reports created by the GRC system can be accessed by the management of a central virtual bank.

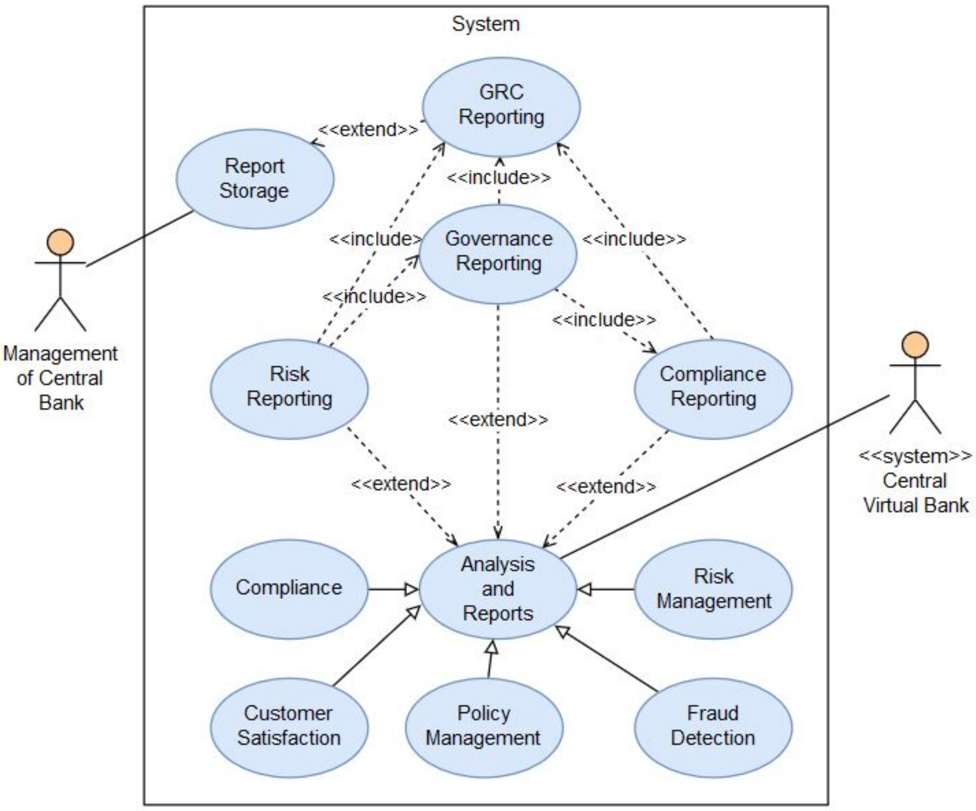


Figure 4.4: Use-case Model of a Central Virtual Bank

Several use-cases about analyses and reports are the same like the ones in the use-case model for a virtual bank. Therefore, it is not necessary to discuss them in detail. New use-models are:

- Governance Reporting: Part of the system related to governance as discussed in detail in chapter 1.1.
- Risk Reporting: All risks from virtual banks are reported here. The risks themselves are described in chapter 1.2.

- Compliance Reporting: An important part of the system where all compliance reports from virtual banks are stored and the results are further processed. Compliance is discussed more in chapter 1.3.

- GRC Reporting: A core component where all parts of the system (governance, risk and compliance) come together.

- Report Storage: A folder where all relevant analyses and reports are stored and accessible to management. The available documents are defined based on the user's role in the system.

4.3 Class Diagram

Based on the information displayed in the use-case models, it is apparent that there is one entity (a central virtual bank in our case) that gathers all information from the rest of the entities (virtual banks) in an integrated set. Therefore, as displayed 4.5, the core class of central virtual bank information is the middle of the scheme, getting all information from virtual banks and creating an analysis based on that data. The data is categorized and processed and reports are generated.

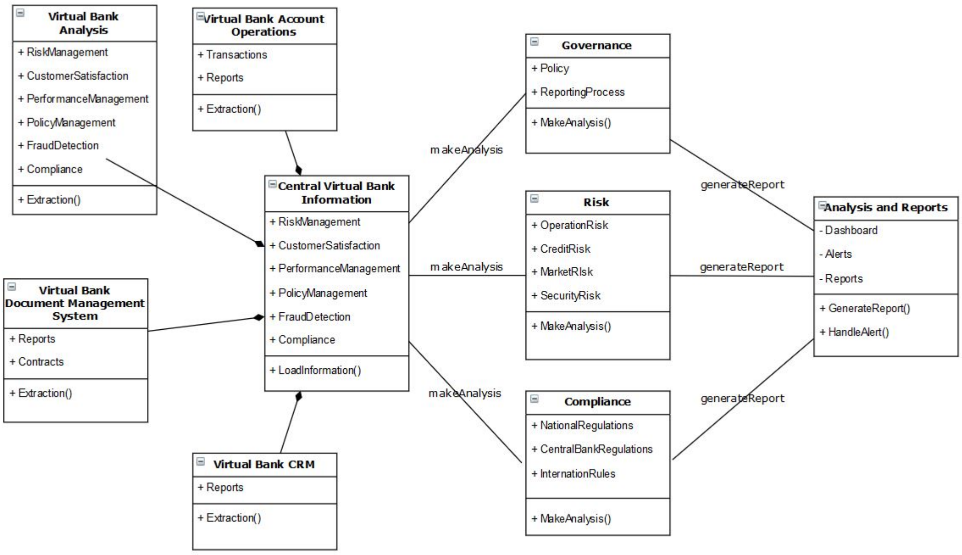


Figure 4.5: Class Diagram

The class diagram contains following classes:

- Central Virtual Bank Information: A core class where data from all virtual banks are being stored. Several actions are being performed using the data such as fraud checks, if compliance requirements were fulfilled or if customer satisfaction were at an acceptable level.

- Virtual Bank Account Operations: A class covering all possible transactions. In our simplified case, it would be just transactions between different bank accounts, but in a more complex case, it would cover loans and investments.
- Virtual Bank Analysis: This class is to some extent similar to central virtual bank information, but it covers information just for one affiliate.
- Virtual Bank Document Management System: Document storage for one affiliate and all of the local reports and analyses are stored here.
- Virtual Bank CRM: Customer Relationship Management for one affiliate containing information about all customers.
- Governance: A class covering processes within the bank.
- Risk: A class implementing risk management.
- Compliance: A class controlling all compliance requirements, not just at an international level, but also at a national level.
- Analysis and Reports: Generated reports are stored in this class and displayed in dashboards. There is alert management as part of this class, therefore, if the compliance requirements have not been fulfilled, relevant people are informed about it.

4.4 Service Workflow

To demonstrate the implementation of a GRC system into an internal infrastructure, a service workflow diagram was created. Consider, for example, the case used in the previous part of this chapter, a central virtual bank. There is an internal user from management, entering the system through their computer and accessing the system via a browser. After successful authentication, the user can use several internal applications either on the intranet or a B2B portal. The GRC system itself is located behind these portals and is accessible via interfaces.

There are three main components inside the GRC system:

- Governance: A part of the system that controls processes within the organization. It includes tools to create new processes as well as editing current ones. Since we are on the level of a central virtual bank, we should be able to watch over the processes of virtual banks.

- Risk: A component to control and mitigate risks. The whole process from identifying risk, its evaluation and subsequent monitoring is present here.
- Compliance: The last component to handle compliance processes and monitor if everything is done within the rules defined by specific authorities.

In order to be working correctly, a GRC system has to be connected to all virtual banks. It is done via interfaces, where all of the relevant data is being transferred into the system.

4.5 Summary

In this chapter, an idea on how to design a GRC system was introduced. Since true GRC systems are usually fully customized to the needs of clients, a specific case-study was chosen, a purely virtual bank operating in several countries. Each of the branches is operating in their country and all of them are reporting to one central authority, which is a central virtual bank. To fulfill all of the requirements defined by certain authorities, information is centralized in order to lower expenses to comply with all of the restrictions.

Afterwards, by using use-case models, the users of the systems were identified and which functionality has to be covered so users were able to access their accounts and operate with their resources. Since the use-case differs for both roles (a virtual bank and a central virtual bank) the two models where created to cover all of the functions.

The following part of the chapter is to get to a lower level of abstraction to elaborate how the classes can be connected and how the system could work. Basically, each of the banks keep their own data, analyses and reports and are sharing all relevant information needed by the central authority to created overall reports, which can help management to make strategic decisions.

The last part discussed the possibility where to place a GRC system in an organizations' infrastructure. The system is working in the background basically hidden from common users/customers. It collects data from all other internal systems and based on that information, it generates reports.

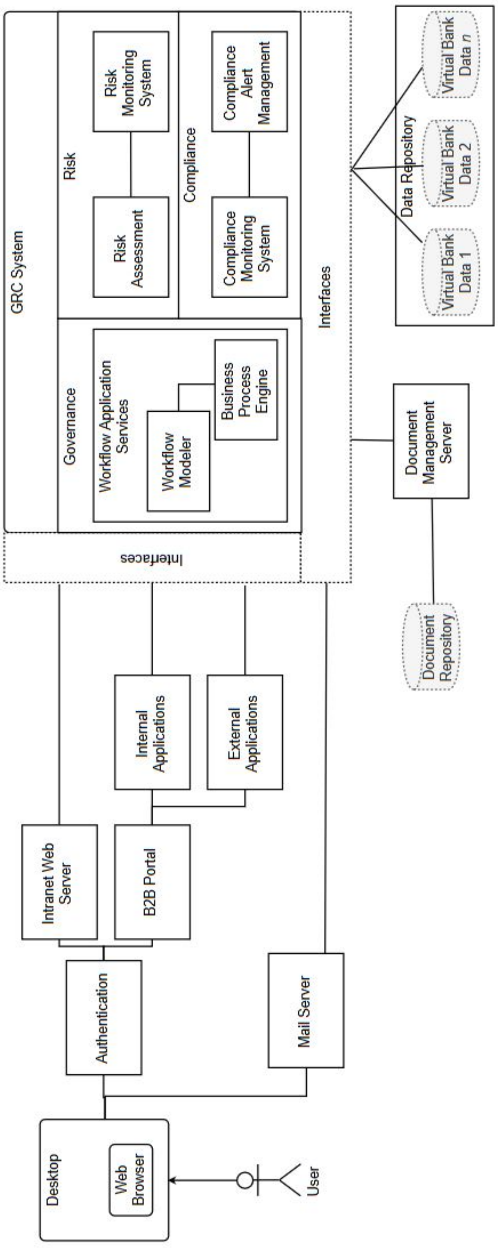


Figure 4.6: Service Workflow Diagram

Chapter 5

Case Study

To demonstrate an implementation of a model-driven GRC system, it was decided to implement a specific process, ideally connected to compliance. To keep pace with the previous chapters, the chosen process is from the financial sector, so it can be connected to a modelled architecture. Therefore, it will continue with a current use-case of virtual banks, where one bank leads the others and stores reports and information about the processes of others banks.

As it was present in the use-case models 4.3 and 4.4 and also in the class diagram 4.5, fraud detection is taken seriously in every bank for obvious reasons, money loss. It is also one of the required processes, so an occurrence of cases such as money laundering is mitigated as much as possible. Therefore, the process to prevent money laundering was chosen to be modelled.

This chapter describes the whole case study step by step:

1. Definition of money laundering: At first it is necessary to describe what money laundering is and what the idea behind it is. Since money laundering is a huge topic, we will consider only part of it.

2. Process modelling: Once the process is described, it is possible to model the process accordingly. For a better image and usability, the process will be situated into an already used use-case of a virtual bank.

3. Process enforcement: One thing is to model the process, but the diagram itself will not prevent money laundering frauds. Therefore, the model has to be deployed into specific software, which allows process enforcement.

5.1 Description of the Money Laundering Process

Before modelling the process, it is necessary to define the gist of it and model the process accordingly. “The term money laundering originates from the US describing the Mafia’s attempt to “launder” illegal money via cash-intensive washing salons, which where controlled by company acquisitions or business formations. Estimated two to five per cent of the global gross domestic product stems from illicit sources. A great deal of the money derives from drug-dealing, with a total revenue of 810 Billion USD in 2003."[42]

"In 2005, the Austrian Police secured drugs worth 49,266,800 Euro (drug seizures in terms of street prices), in total 25,892 people were charged for violating the Austrian Narcotics Act. Most of all illegal transactions are processed by cash since there is the smallest risk to leave one's mark. Nevertheless, an obvious tendency to misuse the Internet in order to undertake illicit transactions in the form of online banking, cyber money and electronic purse exists."[42]

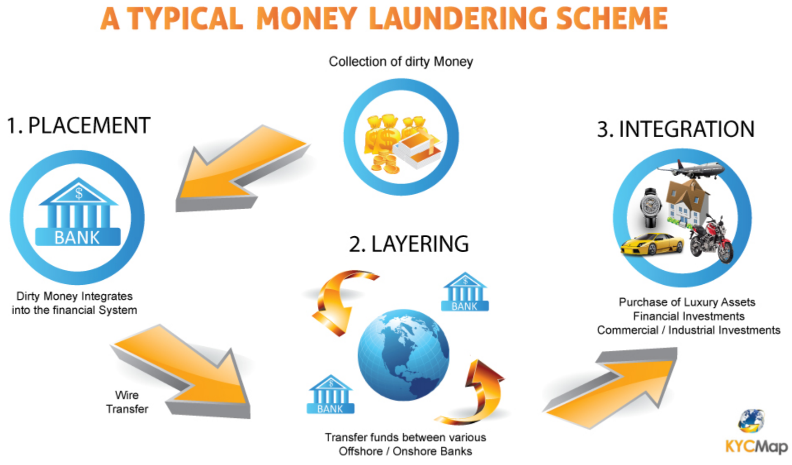

A TYPICAL MONEY LAUNDERING SCHEME
Collection of dirty Money
1. PLACEMENT
BANK
Dirty Money Integrates into the financial System
Wire Transfer
2. LAYERING
BANK
BANK
Transfer funds between various Offshore / Onshore Banks
3. INTEGRATION
Purchase of Luxury Assets
Financial Investments
Commercial / Industrial Investments
KYCMap

Figure 5.1: Money Laundering Scheme [43]

As visible in the previous paragraphs, money laundering is a serious issue, which requires huge investments and many security checks. There are, of course, many approaches on how to prevent such things and each country or financial institution has mechanisms how to prevent these situations [42]. The whole process and idea of money laundering is complicated [44] 5.1, therefore, we will focus on just one part of this process. Each money transfer in our bank triggers a process, where several checks and stakeholders take part. If a money transfer is marked as suspicious, relevant authorities are notified and each case is handled and resolved. The whole process will be described in detail in the following sections.

5.2 Camunda Modeler

To go through the process, software called Camunda Modeler was selected. "It is a desktop application for modeling BPMN workflows and DMN decisions. It is very easy to use, both business analysts and developers can work on the same diagrams. Camunda Modeler supports BPMN 2.0, CMMN 1.1 and DMN 1.1

(including Decision Tables and Decision Requirements Diagrams)."[45] Thanks to additional plugins, it allows the user to simulate the process already in the modeler and test its usability even before deploying it to more sophisticated tools.

In order to fully understand the model, the elements used are defined in the following paragraphs. Only elements which were used in the diagram or elements which were considered will be defined.

5.2.1 Events

BPMN contains several types of events, but just a few of them (5.2) were used in the diagram:

- Start Event: An event used to visualize the beginning of the process.
- End Event: An event used to visualize the end of the process.
- Intermediate Catch Event: This type of event handles triggers. Once this event is reached, this part of the process is put on hold while the token is not received. Afterwards, this process proceeds.

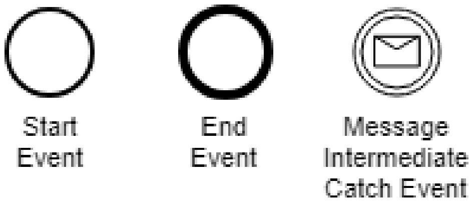


Figure 5.2: Used Types of Events

5.2.2 Tasks

Tasks 5.3 fall among "Activities", which are important components of BPMNs and an atomic part of the process. There are several different types of tasks, such as:

- Service Task: A task which can be used for connecting to an external data source. In Camunda's case, the service task can be accessible via REST API and the task itself can be implemented as a java (or C#) class.
- Send Task: This activity sends a message to another swimline. Once the message is dispatched, the task is completed.

- Receive Task: Represents the opposite function of Send Task. Receive tasks receive messages from other swimlines. Once the message is received, the task is completed.

- User Task: In order to complete this activity, the user needs to perform a specific action. This is usually done with the use of a software application.

- Manual Task: This task is performed without the participation of any business process execution engine or any application.

- Business Rule Task: A task that contains a business rules engine. At the beginning of executing this activity, input data is received and based on the rules and the output data is set.

- Script Task: This task is executed by a business process engine. The behaviour of the task is implemented by a script. Once the script is executed and completed, the activity is also completed.

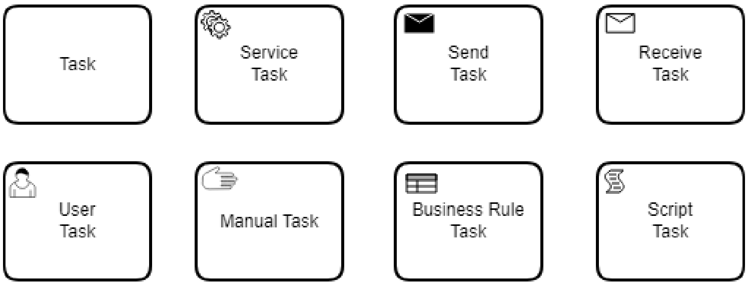


Figure 5.3: Types of Tasks

5.2.3 Gateways

This BPMN component 5.4 is used as a control token flow in a business process. By adding the gateway into the process, the initiation of a different route can be set up. Execution of this component happens at the moment when a token is received and when the token being sent is defined by the gateway itself. A default sequence flow can also be set, so when the needed data is received, the gateway can send a token to a specific sequence flow based on the default flow settings.

Gateways also implement behavior such as process forking (multiple tokens are dispatched) and joining (tokens are received from all incoming sequence flows). There are several different types of gateways, all of which are defined below:

- Inclusive Gateway: A gateway which implements AND/OR behavior. A token from this gateway can be sent to one or multiple sequence flows. It requires a definition of the rules or default sequence flow(s).

- Exclusive Gateway: This gateway implements XOR (exclusive OR) behavior. It means that when a token is received by this gateway, the token is dispatched to just one of the output sequence flows based on internal decision rules. In case that more sequence flows meet the criteria, the first sequence flow which fulfilled the criteria is used.

- Parallel Gateway: A gateway used to fork the process. When it is necessary to send a token to multiple sequence flows simultaneously, a parallel gateway is used. It also offers joining multiple incoming sequence flows. In case of joining processes, the token(s) will be sent once the tokens from all incoming sequence flows are received.

- Event-based Gateway: In this case, when a token is received, the execution of one of the sequence flows is delayed until the subsequent event occurs. If later another subsequent event occurs again, it is ignored since the token was already dispatched. Similar to the case of an exclusive gateway, XOR behavior is implemented. From this event there are always two or more outgoing sequence flows which lead to either an intermediate catch event or a receive task.

- Complex Gateway: This type of gateway can be used for forking or joining complicated processes. It allows the user to freely set rules for incoming and outgoing tokens. However, since the previously mentioned gateways cover most of the situations, complex gateways are not widely used. Also, this type of gateway is not implemented by Camunda Token Simulation. Due to this fact, this component was not used.

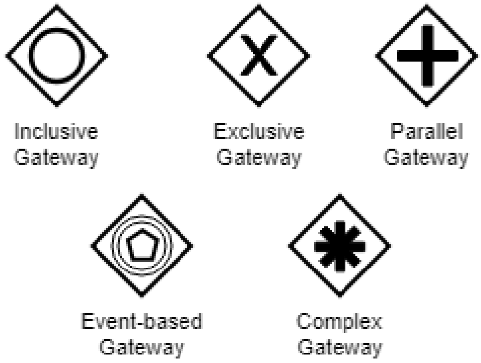
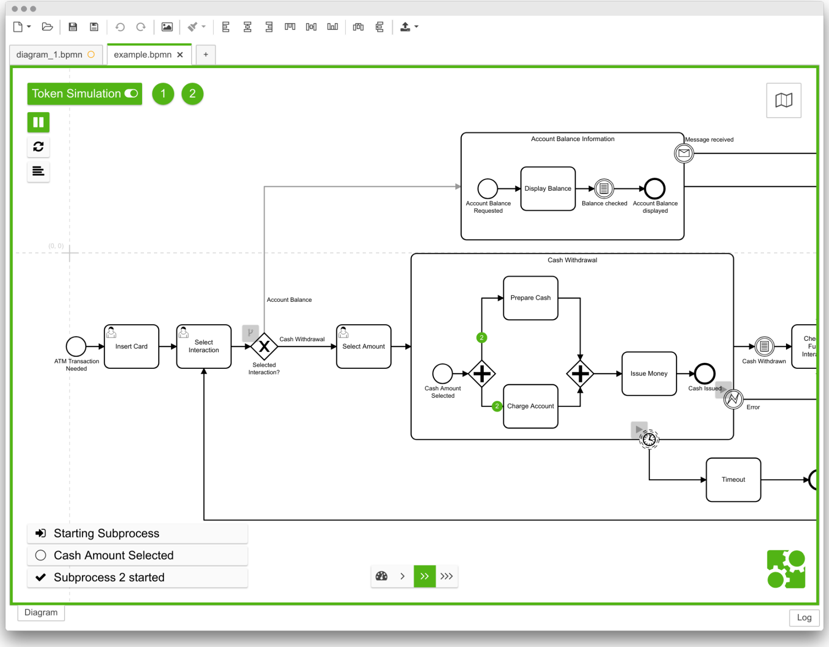


Figure 5.4: Types of Gateways

5.3 Token Simulation Plugin

To execute the process already in the Camunda Modeler, a plugin named “Token simulation as a plugin for the Camunda Modeler” 5.5 was used. It allows users to switch into simulation mode and simulate the token flow. Based on the settings of the gateways tasks, the flow is set accordingly. Thanks to this plugin, it was possible to test the created process diagram already in the modelling process phase.



Starting Subprocess
○ Cash Amount Selected
✓ Subprocess 2 started

Figure 5.5: Token Simulation Plugin for the Camunda Modeler[46]

5.4 Process Modelling

As mentioned, a designed process 5.6 of an anti money laundering mechanism[47] will be evaluating each money transfer based on several criteria which will decide, if the transfer is considered suspicious. Suspicious transfers undergo several additional checks before being finally approved or rejected. An important part of this process is financial authority, which provides data to identify the legal correctness of transfers.

The diagram is divided by swimlines to define the responsibilities of subprocesses. There are three different parties:

1. Client: The role which represents the owner of the bank account (i.e. private person or organization) who initiates the money transfer.
2. Bank: The financial institution which manages the bank account and initiated the money transfer.
3. Financial Authority: The supervisor of the bank defined by the government that needs to cooperate and report specific information.

With all of the roles defined, the money transfer journey can be defined:

- **Client**
  - Process beginning: The start of the whole process.
  - Initiation of money transfer: User activity which through their bank account initiates a money transfer. (5.7)
  - Payment order: By filling in all mandatory data, an order to process the payment is created.
  - Request for additional information: In case a payment is suspicious, information that additional information is needed is received from the bank.
  - Was additional information requested?: An input value for this gateway is set by the previous component. If a message with a request for additional information has not been received, the process continues without additional client input.
  - Provision of requested data: The client is asked to provide the bank with additional information regarding the payment. (5.8)
  - Is the transfer approved?: An event-based gateway which chooses a path according to the message received from bank.
  - Receive transfer confirmation: If the bank confirms the transfer, this information is received.
  - Receive transfer rejection: If the bank rejects the transfer, this information is received.
  - Transfer is executed: After approval from the bank, the payment is executed.
  - Process end: The overall end of the process.
- **Bank**
  - Receipt data with transfer details: The bank receives their first basic information about a money transfer.
  - Does amount exceed specific amount?: Based on the value set by the bank, the payment is evaluated as suspicious.

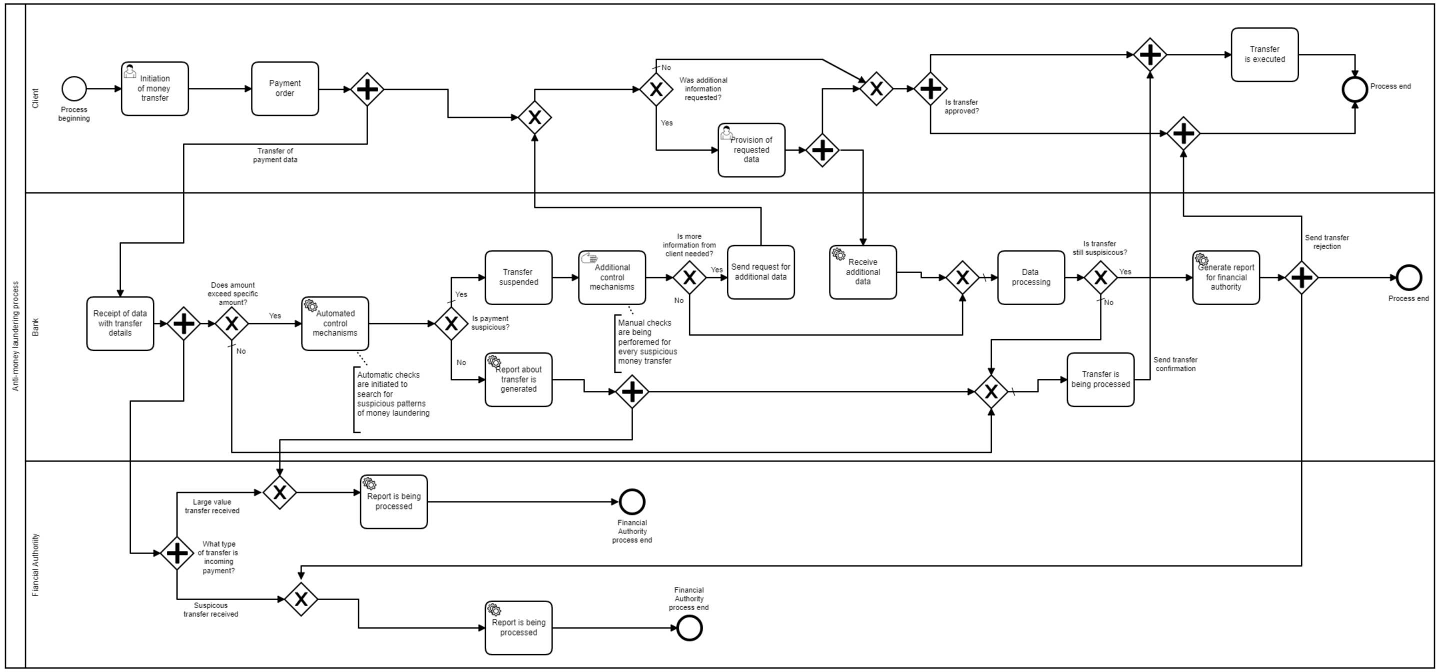
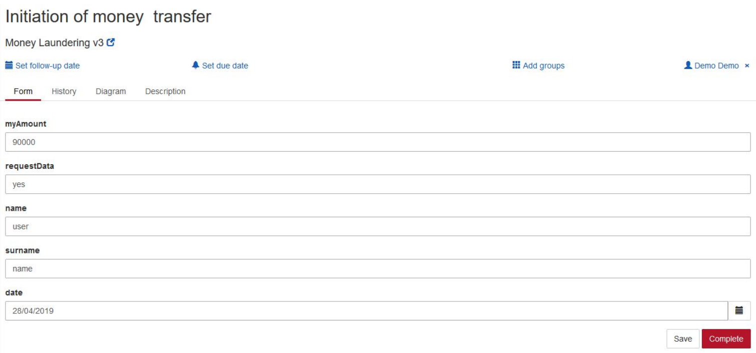

Anti-money laundering process
Client
Bank
Fiancial Authority
Process beginning
Initiation of money transfer
Payment order
Transfer of payment data
Was additional information requested?
No
Yes
Provision of requested data
Is transfer approved?
Transfer is executed
Process end
Receipt of data with transfer details
Does amount exceed specific amount?
Yes
No
Automated control mechanisms
Automatic checks are initiated to search for suspicious patterns of money laundering
Is payment suspicious?
Yes
No
Transfer suspended
Report about transfer is generated
Additional control mechanisms
Manual checks are being perforemed for every suspicious money transfer
Is more information from client needed?
Yes
No
Send request for additional data
Receive additional data
Data processing
Is transfer still suspisicous?
Yes
No
Generate report for financial authority
Send transfer rejection
Process end
Transfer is being processed
Send transfer confirmation
Large value transfer received
What type of transfer is incoming payment?
Suspicous transfer received
Report is being processed
Financial Authority process end
Report is being processed
Financial Authority process end

Figure 5.6: Money Laundering Process


Initiation of money transfer

Money Laundering v3

myAmount: 90000

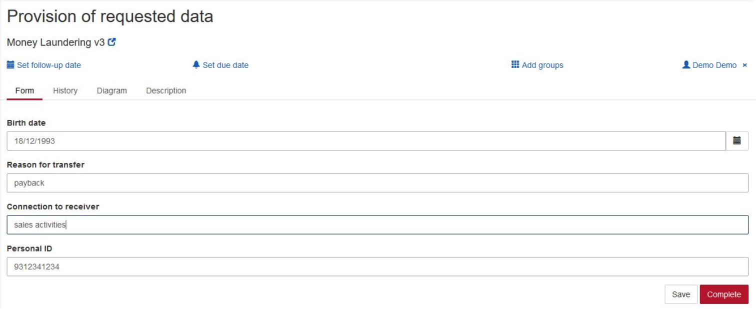
requestData: yes

name: user

surname: name

date: 28/04/2019

Figure 5.7: Form to Initiate Money Transfer in Camunda[39]


Provision of requested data

Money Laundering v3

Birth date: 18/12/1993

Reason for transfer: payback

Connection to receiver: sales activities

Personal ID: 9312341234

Figure 5.8: Form to Provide Additional Data in Camunda[39]

- Automated control mechanisms: A complex step where information about the payment is taken and processed. The goal of this step is to find a pattern in the payment and match it with payments which were already evaluated as a money-laundering case.
- Is payment suspicious?: Based on the results of the previous activity, this gateway is resolved.
- Report about transfer is generated: When the transfer is evaluated as clear, a report about a large value payment is generated and sent to the financial authority.
- Transfer suspended: Once the payment is considered a money-laundering case, it is suspended and further checks are performed.
- Addition control mechanism: A bank employee performs manual steps to check whether the payment is being used for money-laundering. There is the possibility to request additional data (origin of money, information about recipient, etc.).
- Send request for additional data: Based on the decision made during the previous task, a request for additional data is sent.

  - Receive additional data: A task to receive additional data was requested earlier.
  - Data processing: Another round of checks is performed.
  - Is the transfer still suspicious?: Based on the information received during the previous task, a final decision about the transfer is made.
  - Transfer is being processed: The transfer is considered clear and a message about the transfer approval is sent.
  - Generate report for financial authority: A transfer evaluation is finalized and the payment is considered a money-laundering case. A report containing details is generated and sent to the financial authority.

- **Financial Authority**
  - What type of transfer is incoming payment?: A gateway to differentiate between large value transfers and suspicious transfers.
  - Receive large value transfer report: A report created by the bank is received. The goal of the transfer is just to inform and notify the financial authority about the transfer itself. This data is used later for other payments. If one client would be performing several payments such these, they could be asked to prove the origin of the money.
  - Receive suspicious transfer report: The bank evaluated this specific payment as suspicious and stopped its execution. The financial authority is informed.
  - Report is being processed: Further steps of investigation into the client are taken.
  - Financial Authority process end: The end of the process.

5.5 Used Tools: Camunda

When the process is created, it can be uploaded into specialized software, which deploys it and enforces its execution. Camunda was our specialized software in this case. "Camunda is a Java-based framework supporting BPMN for workflow and process automation, CMMN for Case Management and DMN for Business Decision Management."[39] In our case, we will be able to use the diagram created in the previous parts of this chapter and deploy it to Camunda. While deployed in Camunda, we can perform specific actions thanks to its web applications.

There are five different web applications:

- REST API: The REST API allows users to access deployed processes from an external application.

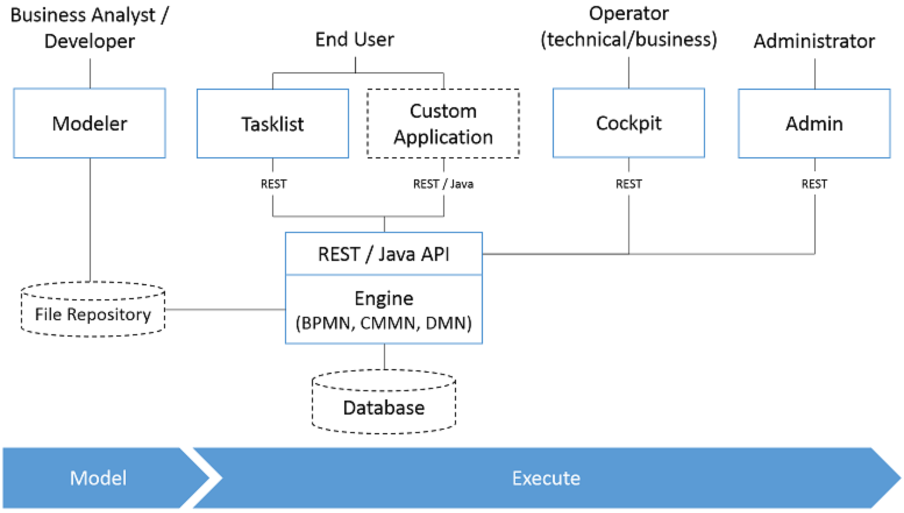


Figure 5.9: Camunda: Architecture Overview[39]

- Camunda Tasklist: Part of the system to support user tasks and allow users to inspect their workflows. It is also possible to perform actions required by tasks by providing the data input. It allows users to claim tasks in order to be able to work on them, to set a follow-up date, to set a due date or even comment on a task.

- Camunda Cockpit: The cockpit provides users mainly with a monitoring option. It is possible to search process instances, check their state or even repair broken instances.

- Camunda Admin: The administration part of the system, further divided into five other environments:

  - User Management: Allows to adding, editing or deleting users.
  - Group Management: The possibility to create or delete groups and add users into these groups.
  - Tenant Management: Similar to group management, this part of the system provides Camunda with functions such as add, edit or delete tenants.
  - Authorization Management: The environment used to set user or group rights for parts of the system.
  - System Management: A simple overview and licence key is present here.

- Camunda Cycle: An application to synchronize BPMN process models between two different systems. For example, it is possible to synchronize a model created in Signavio[48] with a model created in the Camunda Modeler.

5.6 Process Implementation

After the process modelling phase 5.4, it is possible to deploy the model into the workflow engine, in this case Camunda. The BPMN model can be deployed through the graphical user interface, which is present in Camunda or REST API can be used.

```
POST /engine-rest/deployment/create HTTP/1.1
Host: localhost:8080
Content-Type: multipart/form-data; boundary=----
    WebKitFormBoundary7MA4YWxkTrZu0gW
cache-control: no-cache
Postman-Token: 0c638ba5-2faa-4f4e-a383-f4d20e31da55

Content-Disposition: form-data; name="upload"; filename="E:\FIT\MI-DIP
    \camunda\diagram_money_laundering_v3.bpmn
```

Figure 5.10: Model Deployment via REST API

At this moment, the process is deployed in the workflow engine and is ready to be started. Since Camunda has a fairly wide library of functions, which can be called upon via REST API, the whole process can be managed through it. To start the process, another request (5.11) can be sent.

```
POST /engine-rest/process-definition/key/Money_Laundering_v3/start
    HTTP/1.1
Host: localhost:8080
Content-Type: application/json
cache-control: no-cache
Postman-Token: 3ea2603c-5da9-44e7-a50e-ed6b57c91917
{}
```

Figure 5.11: Start of the Process

At this moment, the process has started and since it starts by the “Initiation of a money transfer” task, it is up to the user to perform the requested action, so the process can move on to the further stage. All of the actions are visible in real time in Camunda, therefore, if a user checks the status, they can see the immediate state 5.12.

From the Camunda Cockpit, it is clearly visible that the process had started and was stopped at the “Initiation of a money transfer” task. To perform the user task, it is necessary to send another request 5.13 to REST

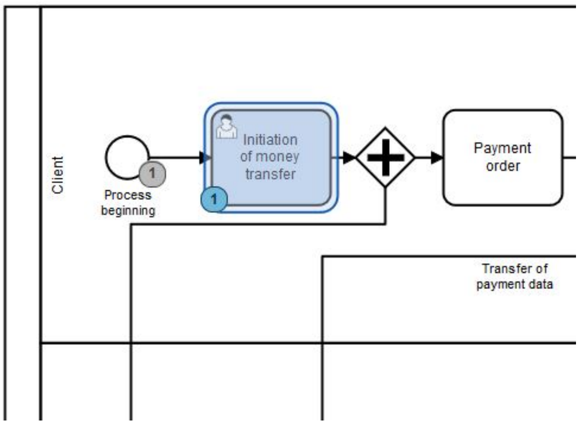


Figure 5.12: Real-time View of an Immediate Process State[39]

API and since it is required to add addition information at this step, several variables need to be defined, so the process can proceed further. At this moment, information about the amount of money, which is being transferred, needs to be attached. Afterwards, the process continuous with the following

```
POST /engine-rest/task/5e1d508f-6153-11e9-992c-8277815642d7/complete
    HTTP/1.1
Host: localhost:8080
Content-Type: application/json
cache-control: no-cache
Postman-Token: bb2adbf1-c5cc-42d7-b315-1934418de402
{"variables":
    {"myAmount": {"value": 4000},
    "name": {"value": "demo"},
    "surname": {"value": "user"},
    "requestData": {"value": "no"},
    "date": {"value": "date"}}
}
```

Figure 5.13: Handling User Tasks

activities and tasks till the end. The whole process can be managed through the API via requests. The status of the process can be seen in the GUI of Camunda, which has several features, which are handy during analysis, like a process heatmap 5.14. The process heatmap highlights the token journey, so it is visible which tasks the process was running and where it was paused. Any created instance of any process is available in the Cockpit and ready to be analyzed and reported.

Two approaches on how to handle the processes were presented (via GUI

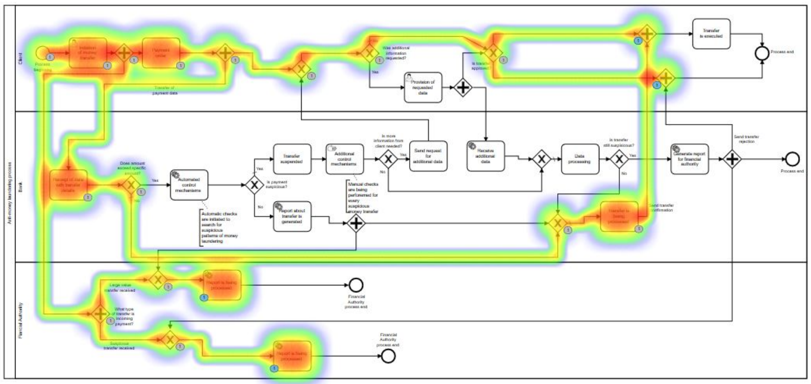

Anti-money laundering process
Client
Bank
Financial Authority
Process beginning
Initiation of money transfer
Payment order
Transfer of payment data
Was additional information requested?
Yes
Provision of requested data
Is transfer approved?
Transfer is executed
Process end
Receipt of data with transfer details
Does amount exceed specific amount?
Yes
No
Automated control mechanisms
Automatic checks are initiated to search for suspicious patterns of money laundering
Is payment suspicious?
Yes
No
Transfer suspended
Report about transfer is generated
Additional control mechanisms
Manual checks are being performed for every suspicious money transfer
Is more information from client needed?
Yes
No
Send request for additional data
Receive additional data
Data processing
Is transfer still suspicious?
Yes
No
Generate report for financial authority
Send transfer rejection
Process end
Transfer is being processed
Send transfer confirmation
Large value transfer received
Report is being processed
Financial Authority process end
What type of transfer is incoming payment?
Suspicious transfer received
Report is being processed
Financial Authority process end

Figure 5.14: Process Heatmap[39]

and REST API), however, there is another way, which would be used in most cases. This is using external classes implemented in a programming language which supports Camunda. Furthermore, implementation in C# will be discussed.

Programming the behavior works in the way that for each task a class is implemented. There is one mandatory variable for each task called a topic name. Based on the topic name, a class can be defined.5.15. When all of the classes are implemented, the program is built and a dll (dynamic link library) file is generated. This file can be used as an input file for a BPM client, which also needs to be implemented in order to simulate the process in this environment. BPM clients work with the dll file and listen to a defined port and address. When there is a task, which is implemented within the dll file, the BPM client takes this task and runs the corresponding function.

```
public class AutomatedChecksAdapter : IExternalTaskAdapter
    {
        public ExternalTaskAdapterInfo MetaData => new
            ExternalTaskAdapterInfo()
        {
            TopicName = "AutomatedChecks"
        };
    ...
```

Figure 5.15: Setup of the Topic Name in C#

As noted above, the whole solution works in a way that at first a connection to Camunda is created by the BPM client and several variables need to be defined to successfully execute the money-laundering process. For the purposes of the test, Camunda is running locally, therefore the base address is “http://localhost:8080/engine-rest”. Once the connection is set up, the

BPMN model can be deployed and the process starts. When the BPM client is running, it is waiting for the address to provide a task, which could be executed. A list of these tasks is defined by the dll file, which was created before. Implementing an external class is only limited by the limitations of the programming language that is implemented, therefore, the code can be fully customized and adjusted according to the programmers needs. As visible in Figure 5.16, a connection to the database can be set up, needed data can be obtained and specific operations can be processed. In the case of the *GenerateEndReportAdapter* class, the program connects to the database, gets information about payments and generates a report based on the payment information.

```
...
MySqlConnection conn;
connetionString = @"Data Source=WIN-50GP30FG075;Initial Catalog=Demodb
    ;User ID=user;Password=pass";
conn = new MySqlConnection(connetionString);
string query = "SELECT * FROM PAYMENTS";
conn.Open();

var cmd = new MySqlCommand(query, conn);
var reader = cmd.ExecuteReader();

while (reader.Read())
{
    var payments = reader["DATA"];
    GenerateEndReport(payments);
}
conn.Close();

return Task.FromResult(result);
...
```

Figure 5.16: Implementation of the Generate End Report Class

5.7 Case Study Summary

To demonstrate the usability of GRC systems, one process was chosen, designed in BPMN and deployed via the workflow engine Camunda. For this matter, the process used to recognize cases of money-laundering by banks was chosen.

At first, the process was described, the gist of money-laundering was discussed and designed in BPMN in the Camunda Modeler. There are of course many different ways how to design such a process, but in the end, there should be three different roles in this process. One is the client or customer, who initiates the money transfer, the second has to be a bank, where the client has opened an account and lastly, there is the financial authority which oversees all large sum or suspicious payments. Thanks to this authority, it is easier for banks to recognize cases of money-laundering. This process has its rules, where based on the transferred amount and account information, it evaluates how the payment proceeds. It even requires the execution of some manual tasks from the bank employee when the transfer is already suspicious after the first round of checks.

All of these cases can be simulated in the Camunda workflow engine, where it is possible to set up different roles, define the initial configuration of the process and start the process afterwards. The process can be controlled via the user interface built-in Camunda, which is quite user-friendly and does not require much technical skill or it can be controlled via REST API or even via an external code written, for example, in C# or Java. The code is used to deploy the BPMN model and to start the process. When the process is running on the server, it can be fully controlled by the user.

This chapter shows the possibilities of the workflow engines and demonstrates the outcome of using these systems to oversee compliance within GRC systems. GRC systems with a built-in workflow engine allow companies to efficiently manage their processes. By using just one system, it would allow companies to centrally oversee all of the processes and changes would be not only be possible, but could also be made quite flexibly.

Conclusion

The goal of this thesis was to investigate the model-driven approach to governance, risk, and compliance systems development and discuss the usability of this approach for companies to lower their operating costs for compliance processes. This main goal was divided into several tasks:

- A review of state-of-the-art GRC platforms: The first two chapters, (Governance, Risk and Compliance and GRC Systems), were devoted to fulfill this task. The GRC system was specified and each of the three main parts of the system were defined. Then whole GRC system was divided into several components and the main vendors were introduced.
- A comparison of the benefits and suitability of GRC platforms, BPM systems, low-code platforms and custom development to support GRC management: A comparison of different platforms was the main aim of chapter 3 – Comparison of Systems, therefore, GRC, BPM and low-code platforms were defined and compared to each other. Due to reasons discussed in that chapter, custom developed was only defined and excluded from the comparison afterwards.
- Proposing suitable software architecture for implementing a GRC system: Chapter 4 – Software Architecture of GRC Systems discusses the possibilities how to implement a GRC system. A case study from the financial sector was chosen and based on this specification a system was designed.
- Create a case study which demonstrates the implementation of a model-driven GRC system in an enterprise: This is basically a continuation of the previous chapter and takes one process from the financial sector and proposes possible implementation. This is discussed in detail in chapter 5 – Case Study, where it begins with a description of the money-laundering process and continues with the design in BPMN and deployment to the wokrflow engine and ends with the implementation

of the process tasks. This chapter also demonstrates the opportunities, how model-driven systems can help companies with the GRC management to reduce their operating costs.

This thesis provides an introduction to the world of GRC systems. Starting with basic theory, through more complicated views on the architecture of these systems, on to the specific process described in detail and implemented. It can be helpful not just for beginners in IT, seeking for knowledge of these systems, but also for more experienced users interested in GRC systems or process modelling.

Future Work

Even though this thesis and process implementation is finished, there are still several areas which can be examined in addition to this thesis.

- Real case study analysis: Possibly the best way to analyze GRC systems would be via a real case study of a solution implemented for a company. However, documentation of these systems is in the vast majority of cases confidential.

- Comparing GRC or BPM systems to custom development: There is an assumption that custom software is more expensive than building it with a low-code platform or GRC system. An analysis of this claim might bring interesting results in terms of the costs of these systems.

- Comparing the implementation of the processes in Camunda with other platforms: There are several other platforms suitable for creating this process, such as Signavio[48]. The platforms could be compared and their advantages and disadvantages could be explored.

Bibliography

[1] Berwin Leighton Paisner. The speed of business: Innovation, business growth and the impact of regulations [online]. 2018, [Accessed: 07-12-2018]. Available from: `https://www.blplaw.com/media/know-how/speed-of-business/BLP_The-Speed-of-Business-impact-of-regulation.pdf`

[2] Papazafeiropoulou, K., A. Spanaki. Understanding governance, risk and compliance information systems (GRC IS): The experts view. 2015, doi: 10.1007/s10796-015-9572-3.

[3] ISACA Monterrey. Governance, Risk and Compliance [online]. 2019, [Accessed: 05-03-2019]. Available from: `https://www.isaca.org/chapters7/Monterrey/Events/Documents/20132305%20Governance,%20Risk%20and%20Compliance.pdf`

[4] Racz, N.; Weippl, E. R.; Seufert, A. A process model for integrated IT governance , risk , and compliance management. 2010.

[5] KPMG International. *The cost of compliance [online]. 2018, [Accessed: 28-12-2018].* Available from: `https://home.kpmg.com/content/dam/kpmg/pdf/2014/07/Cost-of-Compliance.pdf`

[6] Forrester Research, Inc. Governance, Risk and Compliance [online]. 2018, [Accessed: 14-12-2018]. Available from: `https://www.logicmanager.com/forrester-wave-grc-platforms-2018/`

[7] Murphy, R.; O'Malley, C. The Forrester Wave$^{\mathrm{TM}}$: Governance, Risk, And Compliance Platforms, Q1 2018. 2018.

[8] W., V. G. *Introduction to the minitrack IT Governance and its Mechanisms, Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS).* 2002.

[9] *The American Heritage dictionary.* Houghton Mifflin, 1991.

[10] Institute, I. G. *Board Briefing on IT Governance 2nd Edition.* 2003, ISBN 1-893209-64-4.

[11] OGC. *The Official Introduction to the ITIL Service Lifecycle.* TSO, 2007.

[12] Haes, W., S.D.; Grembergen. *Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5 (2nd ed.).* Springer, 2015, ISBN 978-3-319-14547-1.

[13] ISO/IEC 27000 family - Information security management systems. 2019. Available from: `https://www.iso.org/isoiec-27001-information-security.html`

[14] S. Halliday, R. v. S., K. Badenhorst. *A business approach to effective information technology risk analysis and management.* 1996.

[15] K. Bandyopadhyay, K. M., P.P. Mykytyn. *A framework for integrated risk management in information technology.* 1999.

[16] *ISO 31000: 2018, Risk management - guidelines.* International Organization for Standardization, 2018.

[17] smartsheet. Maintain, Protect, and Diminish Risk with a Comprehensive IT Compliance Strategy [online]. 2019, [Accessed: 21-03-2019]. Available from: `https://www.smartsheet.com/understanding-it-compliance`

[18] European Parliament and the Council of the European Union. Regulation (EU) no 2016/679. 2016. Available from: `https://eur-lex.europa.eu/eli/reg/2016/679/oj`

[19] BIS. Basel III: international regulatory framework for banks. 2019. Available from: `https://www.bis.org/bcbs/basel3.htm`

[20] Mania, M. SOX (Sarbanes-Oxley Act) [online]. 2019, [Accessed: 06-03-2019]. Available from: `https://managementmania.com/cs/sox-sarbanes-oxley-act`

[21] HHS. Summary of the HIPAA Security Rule [online]. 2019, [Accessed: 06-03-2019]. Available from: `https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html`

[22] PCI. PCI Security [online]. 2019, [Accessed: 06-03-2019]. Available from: `https://www.pcisecuritystandards.org/pci_security/`

[23] Herbsleb, J.; Zubrow, D.; Goldenson, D.; et al. Software Quality and the Capability Maturity Model. *Communications of the ACM*, volume 40, 06 1997, doi:10.1145/255656.255692.

[24] Paul, M.; Curtis, B.; Chrissis, M.; et al. *Capability Maturity Model for Software, Version 1.1.* 01 1993, 7-14 pp.

[25] Mitchell, S. *GRC Capability Model (Red Book) in Paperback.* OCEG GRC series, Lulu.com, 2017, ISBN 9781300902881.

[26] Mitchell, S. L.; Switzer, C. S. *GRC capability model version 3.0;.* OCEG, 2015.

[27] LogicManager. Identify and Assess Risk [online]. 2019, [Accessed: 26-03-2019]. Available from: `https://www.logicmanager.com/erm-software/product/assess/`

[28] MetricStream. Leading Global Bank Improves Internal Audit Efficiency Through an Automated, Risk-based Approach [online]. 2019, [Accessed: 16-01-2019]. 2018. Available from: `https://www.metricstream.com/casestudy/global-bank-improves-internal-audit.htm`

[29] MetricStream. One of India's Largest Chemical Manufacturers Achieves an Integrated, Enterprise-wide View of Compliance across Multiple Central and State Regulations [online]. 2019, [Accessed: 16-01-2019]. Available from: `https://www.metricstream.com/casestudy/chemical-manufacturers-compliance.htm`

[30] MetricStream. Leading Entertainment and Media Corporation Adopts a Holistic Approach to Social Compliance Management across Thousands of Factories Worldwide [online]. 2019, [Accessed: 16-01-2019]. Available from: `https://www.metricstream.com/casestudy/social-compliance-mgmt.htm`

[31] BPM. What is BPM [online]. 2019, [Accessed: 18-03-2019]. Available from: `http://bpm.com/what-is-bpm`

[32] Dumas M., M. J. R. H. A., La Rosa M. *Introduction to business process management. In Fundamentals of Business Process Management (pp. 1-31).* Springer, 2013.

[33] PEGA. Pega Platform [online]. 2019, [Accessed: 11-04-2019]. Available from: `https://www1.pega.com/products/pega-platform`

[34] IBM. IBM Business Process Management [online]. 2019, [Accessed: 10-04-2019]. Available from: `https://www.ibm.com/cloud/automation-software/businessprocess-management`

[35] Richardson, C. The Forrester Wave$^{\mathrm{TM}}$: BPM Platforms For Digital Business, Q4 2015. 2015.

[36] Rymer, J. R. The Forrester Wave^{TM}: Low-Code Development Platforms For ADD Pros, Q4 2017. 2017.

[37] Appian. Low-Code Development [online]. 2019, [Accessed: 27-02-2019]. Available from: `https://www.appian.com/platform/low-code/`

[38] SoftExpert. Software for Business Management [online]. 2019, [Accessed: 02-04-2019]. 2019. Available from: `https://www.softexpert.com/solucao/business-process-management-bpm/`

[39] Camunda. Camunda Docs [online]. 2019, [Accessed: 08-02-2019]. Available from: `https://docs.camunda.org/manual/7.7/introduction/`

[40] ScienceSoft. Sharepoint Document management system demo [online]. 2019, [Accessed: 11-03-2019]. Available from: `https://www.scnsoft.com/services/sharepoint/document-management/demo`

[41] Ahmadalinejad, M.; Hashemi, S. M. A National Model to Supervise on Virtual Banking Systems through the Bank 2.0 Approach. *advances in computer science : an international journal*, volume 4, 01 2015: pp. 83–93.

[42] Schneider, F.; Windischbauer, U. Money Laundering: Some Facts. *European Journal of Law and Economics*, volume 26, 02 2008: pp. 387–404, doi:10.1007/s10657-008-9070-x.

[43] KYCMap. What is Money Laundering? The Three Stages in Money Laundering... [online]. 2019, [Accessed: 10-04-2019]. Available from: `http://kycmap.com/what-is-money-laundering/`

[44] FATF. Professional Money Laundering [online]. 2019, [Accessed: 07-04-2019]. Available from: `www.fatf-gafi.org/publications/methodandtrends/documents/professional-money-laundering.html`

[45] Camunda. Modeler [online]. 2019, [Accessed: 20-03-2019]. Available from: `https://camunda.com/products/modeler/`

[46] barmac. Token simulation as a plugin for the Camunda Modeler [online]. 2019, [Accessed: 20-03-2019]. Available from: `https://github.com/bpmn-io/bpmn-js-token-simulation-plugin`

[47] Barnawi, A.; Awad, A.; Elgammal, A.; et al. Runtime self-monitoring approach of business process compliance in cloud environments. *Cluster Computing*, 10 2015, doi:10.1007/s10586-015-0494-0.

[48] Signavio. Signavio. 2019. Available from: `https://www.signavio.com/`

Appendix A

Acronyms

API Application Programming Interface

BPM Business Process Management

BPMN Business Process Model and Notation

CMM Capability Maturity Model

CRM Customer Relationship Management

GUI Graphical User Interface

GRC Governance, Risk, Compliance

REST Representational State Transfer

SQL Structured Query Language

URL Uniform Resource Locator

Appendix B

Installation Guide

B.1 Requirements

- Camunda Enterpise Platform 7.10.0-ee (or higher)
- Microsoft Visual Studio with following packages downloaded:
  - Ei.BPM.Client v1.0.4
  - MySQL.Data v8.0.15
  - NETStandard.Library v2.0.3

B.2 Execution

1. Build the project MoneyLaunderingProcess.csproj.
2. Copy generated .dll file from MoneyLaundering.Process\bin folder into the MoneyLaundering.BpmClientTest\bin\Debug\Plugins folder.
3. Run the MoneyLaundering.BPMClientTest application.
4. Deploy the BPMN model in Camunda Cockpit environment.
5. Start the process from Camunda Tasklist.

After the start of the application via Visual Studio, command line window appears with the message that server is running. From now on, any task which topic name matches with the available functions is executed.

Appendix C

Contents of CD

- `readme.txt` .... the file with CD contents description
- `exe` .... the directory with executables
- `src` .... the directory of source codes
  - `implementation` .... implementation sources
    - `MoneyLaundering_BPMClientTest` .... implementation of client
    - `MoneyLaundering_Process` .... implementation of tasks
  - `thesis` .... the directory of LaTeX source codes of the thesis
- `text` .... the thesis text directory
  - `MT_Muzak_Martin_2019.pdf` .... the thesis text in PDF format
  - `thesis.ps` .... the thesis text in PS format