

Jonne Heiniemi

How to implement integrated GRC with RSA Archer

Project guide utilizing RAD model

How to implement integrated GRC with RSA Archer

Project guide utilizing RAD model

Jonne Heiniemi
Bachelor's thesis
Spring 2018
Tietojenkäsittelyn tutkinto-ohjelma
Oulu university of applied sciences

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietojenkäsittelyn tutkinto-ohjelma, Järjestelmäasiantuntija

Tekijä(t): Jonne Heiniemi

Opinnäytetyön nimi: How to implement integrated GRC with RSA Archer

Työn ohjaaja: Teppo Räisänen

Työn valmistumislukukausi ja -vuosi: Kevät 2018

Sivumäärä: 49 + 5

Työssä tutkitaan mitä on hyvä hallinnointitapa, riskinhallinta ja säädöstenmukaisuus. Työ tutkii miten nämä käsitteet toimivat käytännössä ja luo ohjeen, kuinka ne sulautetaan saman järjestelmän alle projektissa. Työn tarkoituksena on lisätä omaa ja muiden ymmärrystä kokonaisuudesta, josta ei ole tarjolla käytännön oppaita.

Järjestelmänä käytetään RSA Archeria ja projektinhallintaan käytetään nopean kehityksen mallia jossa ei käydä läpi henkilörooleja tai liiketoimintapauksen määrittelyä. Työssä käydään läpi koko nopean kehityksen mallin kehityselinkaari.

Menetelmänä toimii konstruktiiivinen tutkimus, joka vuorottelee teorian ja käytännön välillä. Tietoperustana toimii kirjallinen perusta aiheeseen liittyvistä asiakirjoista ja käytännöllinen perusta käytetystä sovelluksesta, RSA Archerista

Työn aihe valikoitu siksi, koska se vastaa työnkuvaani ja tämän työn myötä uskon olevani parempi työssäni. Työn tarkoituksena on lisätä omaa ja muiden ymmärrystä kokonaisuudesta, josta ei ole tarjolla käytännön oppaita.

Työn toimeksiantaja on Governify Oy, jossa minä, työn tekijä työskentelen konsulttina.

Asiasanat: GRC, vaatimustenmukaisuus, hallintotapa, riskinhallinta, projektinhallinta, RSA Archer, opas

ABSTRACT

Oulu University of Applied Sciences
Business Information Technology, System administration

Author(s): Jonne Heiniemi

Title of thesis: How to implement integrated GRC with RSA Archer

Supervisor(s): Teppo Räsänen

Term and year when the thesis was submitted: Spring 2018 Number of pages: 49 + 5

Thesis examines what is good governance, risk management and compliance. It explains how they work in practice and how they can be integrated under the same platform in a project. The purpose of this thesis is to add to my own knowledge about the subject and also help others understand the subject better. There are no simplified guides available about the topic.

The system used is RSA Archer and the project management utilizes rapid application development model without roles and business case definition. Thesis goes through the entire rapid application development life cycle.

Methodology chosen is a constructive research which takes turns between theory and practice. Theoretical foundation of the subject is based on both empirical and practical knowledge. Empirical knowledge is acquired from related documents and practical knowledge is acquired from using the software RSA Archer

Topic was chosen because it reflects to my work description and I believe that after this thesis I am better at my work. Thesis is significant to me and everyone else who tries to understand the concept of governance, risk management and compliance.

Topic was assigned to me by Governify Oy, where I, the author work as a consultant.

Keywords: GRC, governance, compliance, risk management, project management, guide

TABLE OF CONTENTS

| | | |
|-------|---|----|
| 1 | INTRODUCTION | 7 |
| 1.1 | RAD Methodology | 8 |
| 1.2 | RSA Archer | 9 |
| 2 | WHAT IS GRC..... | 11 |
| 2.1 | Governance..... | 11 |
| 2.1.1 | Organization structure..... | 12 |
| 2.1.2 | Strategy & Objectives | 12 |
| 2.1.3 | Responsibility..... | 13 |
| 2.2 | Risk Management | 13 |
| 2.2.1 | Risk management as a process..... | 14 |
| 2.2.2 | Framework..... | 15 |
| 2.2.3 | Principles & Internal Auditing | 16 |
| 2.3 | Compliance | 16 |
| 2.3.1 | Compliance Program | 17 |
| 2.3.2 | Reporting | 17 |
| 3 | REQUIREMENTS PLANNING..... | 18 |
| 3.1 | Research current situation..... | 18 |
| 3.1.1 | Program scope..... | 18 |
| 3.1.2 | Maturity assessment | 19 |
| 3.2 | Define & Finalize requirements | 22 |
| 4 | USER DESIGN..... | 24 |
| 4.1 | System Area Model & System design | 24 |
| 4.1.1 | Archer data visualization elements | 25 |
| 4.1.2 | Archer data configuration elements | 28 |
| 4.2 | Prepare implementation strategies & refine system design..... | 32 |
| 4.3 | Finalize & Approve system design | 32 |
| 5 | RAPID CONSTRUCTION..... | 34 |
| 5.1 | Preparing for rapid construction | 34 |
| 5.2 | System construction | 35 |
| 5.3 | Generating test data & system documents..... | 35 |
| 5.3.1 | Test Plan & Data..... | 35 |

| | | |
|-------|--|----|
| 5.3.2 | Manuals & Technical Documentation..... | 37 |
| 5.4 | Preparing for transition | 37 |
| 5.4.1 | Data Conversion | 37 |
| 5.4.2 | Packaging | 38 |
| 5.4.3 | Training plan | 39 |
| 5.5 | Verifying system construction..... | 39 |
| 6 | TRANSITION..... | 41 |
| 7 | CONCLUSION..... | 42 |
| | REFERENCES | 44 |
| | APPENDICES..... | 50 |

1 INTRODUCTION

This constructive research examines what is GRC (Governance, Risk Management & Compliance) and how do you implement it properly, in this case specifically with RSA Archer platform. Main components include explaining the main concepts of GRC, investigating the requirements planning and design process for GRC project and finally GRC implementation and transition process with RSA Archer GRC Platform. Research is examining the topic on high level meaning that budgeting and detailed project participant tasks are left out of scope. The focus is in understanding the theory and technology that enables integrated GRC, rather than in examining the individual roles or how to create business case.

The objective of this thesis is to lower the bar of understanding what GRC is and give basic understanding how to implement it. Currently the available information is either fragmented, or it requires very in-depth knowledge of the topic. This thesis should help in enabling people and organizations who are not very familiar with GRC or GRC development projects by hopefully simplifying the concept with a development project walkthrough. This walkthrough is displayed using Rapid Application Development (RAD) life cycle.

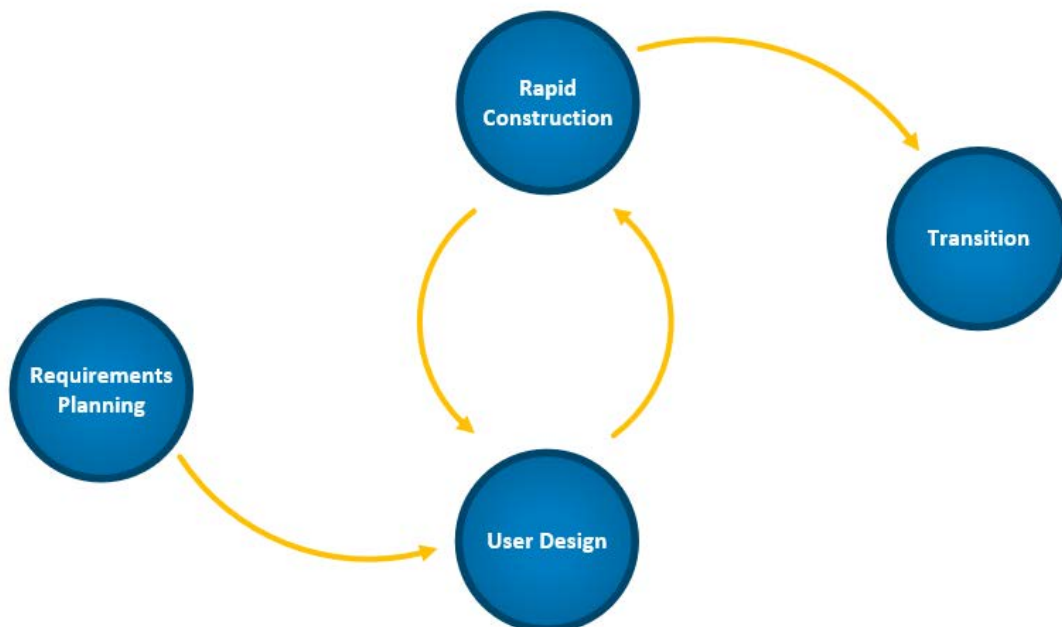


FIGURE 1. RAD Life cycle

Theoretical foundation of the subject is based on both empirical and practical knowledge. As GRC is still a young concept and RSA Archer GRC Platform is a very specific tool to solve the problem the theoretical foundation is largely based on articles, scientific journals, RSA Archer brochures and RSA Archer technical specification documents. The constructive research is divided into Subject orientation and explaining the project phases by RAD structure.

Practical part of this thesis is conducted using RSA Archer (sometimes referred to as RSA Archer GRC platform) which will showcase the benefits and features of a dedicated GRC tool in action.

The topic was chosen to strengthen my knowledge foundation on GRC and development projects which will help me directly in my work life. Purpose of this thesis is to give a realistic view with a practical approach on software development project. The results of this thesis can be applied in practice and work life by myself and anyone interested in GRC.

Thesis is conducted for Governify Ltd where I, the author, also work as an GRC platform/Archer consultant. Governify is a GRC consultancy company based in Finland offering services on EMEA (Europe, Middle-East & Africa) region. Governify is an official RSA partner. From Governify's perspective the research can be used to improve people's GRC awareness by collecting essential information in the same place.

1.1 RAD Methodology

This thesis examines using of Rapid Application Development methodology in GRC project. To fully understand the benefits of RAD, it is essential to know what the methodology of RAD is. RAD is a type of methodology that does not spend a lot of time in initial planning and instead uses a prototyping method to complete the project. (HKSAR 2009, cited 29.5.2018.)

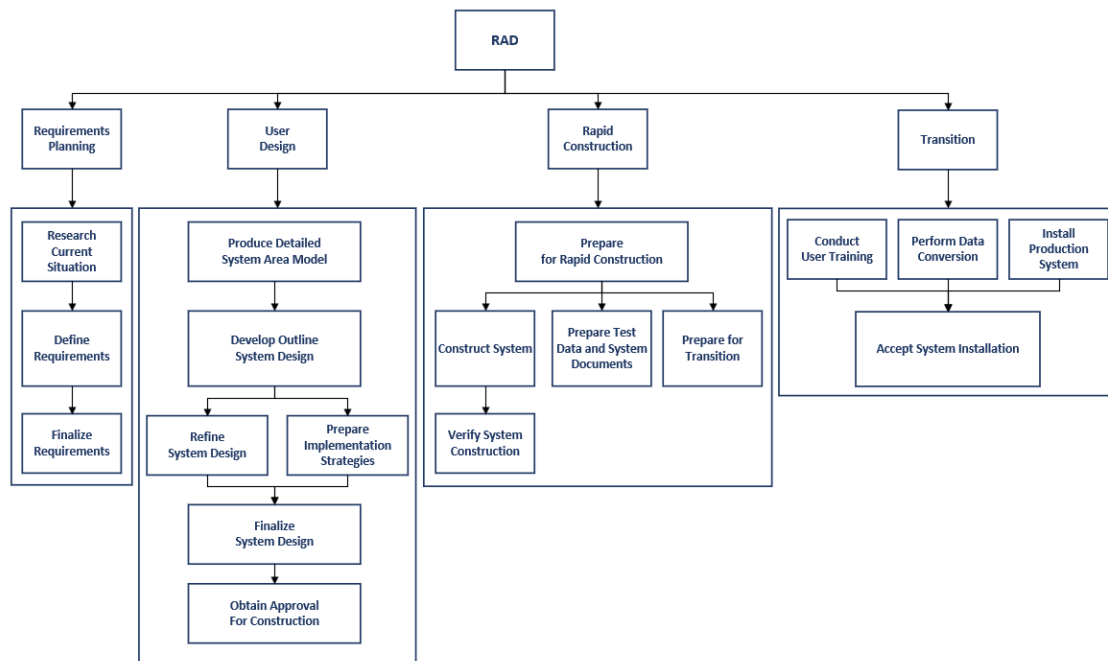


FIGURE 2. Entire RAD Structure

RAD structure is divided into tasks and subtasks which can be seen in the figure 2. This structure also forms a clear structure for the practical part of this research (HKSAR 2009, cited 29.5.2018). Related major RAD techniques are introduced in the thesis as they are used.

The most significant feature of RAD is the endless iteration between user design phase and rapid construction phase. In practice this means that design is refined and the system is tested over and over again until it meets all the requirements. More requirements can be assigned at any iteration. (HKSAR 2009, cited 29.5.2018.)

RAD model suits well for the project if the development can be divided into clear modules, meaning that new requirements do not require the entire system to be built again from scratch (Gimon, cited 31.5.2018).

1.2 RSA Archer

The RSA Archer GRC platform supports GRC management at the enterprise level. As the foundation for all RSA Archer GRC solutions, the platform allows organizations to adapt a wide range of solutions to their needs, create new business processes and integrate with external systems without touching a single line of code. (RSA Security LLC 2018a, cited 24.3.2018.) RSA

Archer's strategy has convinced some of the Fortune 500 companies, like Shell (RSA Security LLC 2018b, cited 24.5.2018). These companies have seized the power of the platform to take advantage of RSA Archer solutions and model additional business processes in part of the time required to develop traditional custom applications (RSA Security LLC 2018a, cited 24.3.2018).

RSA Archer has a very flexible and modular structure. The modular structure is designed to achieve a platform that can be configured to satisfy every customer's needs. RSA Archer's high level of configurability, easiness for end user, and modern and simple look help GRC professionals to execute effectively instead of lacking speed in their workflow. It also provides assurance and confidence in an enterprise's risk management and overview that the executives require in today's environment (Gelnow & Marden 2017, cited 2.4.2018).

This thesis uses RSA Archer version 6.3 for examining the features.

2 WHAT IS GRC

GRC is a broad concept to understand and explain. The acronym originates from words Governance, Risk Management and Compliance. Basically, GRC is a collection of critical functions that perform better together. Some key elements include organization structure, policy management, responsibility, risk as a process, risk management framework, internal audit, laws & regulations, compliance issue management and reporting. (OCEG, cited 17.3.2018.)

One way to understand GRC better is to completely switch the context you are looking at it from. In practice GRC is nothing revolutionary (OCEG, cited 17.3.2018). It is part of human nature and it has been so since the dawn of time. To elaborate this in an example, humans gathered together to form tribes because it brought safety, i.e. humans gathered to manage the common risks. When tribe grew bigger a chieftain came to power to govern the tribe. Eventually common rules were put to place which the population was expected to comply. Fast-forward some hundreds of years and these rules evolved into laws & regulations which have controlled organizations and companies since the beginning. (RSA 2017b, cited 2.6.2018.)

There are several contenders who take credit for inventing GRC as we know it now. However, the first academic research that discusses today's GRC is from 2007, GRC360: A framework to help organizations drive principled performance, written by Scott L. Mitchell. (OCEG, cited 17.3.2018.)

2.1 Governance

Governance is a process of decision making (Sheng 2009, cited 16.5.2018). Governance should define how the organization is led. It should define organizations business hierarchy, goals and objectives. Governance is a very broad concept and in the context of GRC it is usually either IT governance or corporate governance.

Corporate governance is essentially about reconciling the interests of many stakeholders in a company such as shareholders, management, customers, suppliers, financiers, government and society. Most companies strive for a high level of corporate governance: For many shareholders, it is no longer enough for a company to just make profit. Now it must also demonstrate a good social

conscience through environmental awareness, ethical behavior and by practicing responsible corporate governance. Governance defines how the business is managed whether that is for good or bad. (Investopedia. 2018a, cited 2.4.2018.)

2.1.1 Organization structure

Process based organization divides its layers into horizontal layers which emphasize and clarify relationships between functions (Hernaus 2008, cited 23.3.2018).

To understand these layers organization has to look processes on three different perspectives: organizational level, unit level and individual level. From here three different main levels can be identified for the organization structure; board of directors, management and finally process teams. This will result in more flexible, adaptive, and responsive organization structure, meaning it is also more involved. This way it will help organization tackle coordination problems in increase effectiveness and efficiency. (Hernaus 2008, cited 23.3.2018.)

2.1.2 Strategy & Objectives

One important aspect of Governance is that it sets the way organization or entity is doing business meaning it has to be consensus oriented and comprehensive. Basis for establishing this are organization's mission, vision and core values. The mission defines what is the purpose and meaning of the organization. Vision sets out to understand how the organization or entity will look in the future. For example, bank's mission can be providing banking services but vision could be providing banking services globally. Core values then define what kind of measures organization is willing to use to achieve its mission and vision. In order to achieve new goals, the organization forms a strategy and creates objectives to establish a path to follow. (PwC 2016, cited 24.4.2018.)

The management defines the strategy and integrates it into the business activities. At the company or enterprise level, business objectives are set, strategies defined and decisions made on the use and management of resources. From an IT point of view, company-wide guidelines and other guidelines are defined and communicated throughout the organization. These actions are usually based on best practices, standards and regulations. (IT Governance Institute 2006, cited 23.3.2018.)

Strategy and objectives also give direction to risk management and compliance. By setting its mission, vision and core values the organization will take its first step defining what kind of risks it is willing to accept. (PwC 2016, cited 24.4.2018.).

2.1.3 Responsibility

To achieve good governance the organization's governance should be consensus oriented and comprehensive, involved and responsive. It should also be effective and efficient, accountable, transparent, just and follow the laws and regulations (Sheng 2009, cited 16.5.2018)

Usually this can be established with ethical behavior and maintaining integrity but if things go wrong someone has to step up. Necessary part of governance is to take responsibility. Making choices on which standards and policies to comply it is important to understand that this can reflect on organizations image. (Corlett Bolton & Co 2003. Cited 24.3.2018.)

2.2 Risk Management

Risk management is a process of reactively dealing with problems once they arise. Organization should thrive to manage all risks (ISO/IEC 2009, 6). The importance of organized and adequate risk management was realized in the wake of the financial crisis of 2008. Since that time, new risk management standards have been published, including the international standard ISO 31000 for Risk management (Bird 2009, cited 20.4.2018). There are many ways to define risk and risk management. Risk management means understanding, analyzing and managing risks to ensure that organization will achieve its goals. (AIRMIC, Alarm, IRM 2010, cited 2.4.2018.).

The definition set out in ISO Guide 73 is that risk is the "effect of uncertainty on objectives". In order to assist with the application of this definition, Guide 73 also states that an effect may be positive, negative or a deviation from the expected, and that risk is often described by an event, a change in circumstances or a consequence. This definition links risks to objectives. Therefore, this definition of risk can most easily be applied when the objectives of the organization are comprehensive and fully stated. Even when fully stated, the objectives themselves need to be challenged and the assumptions on which they are based should be tested, as part of the risk management process. (AIRMIC, Alarm, IRM 2010, cited 2.4.2018.)

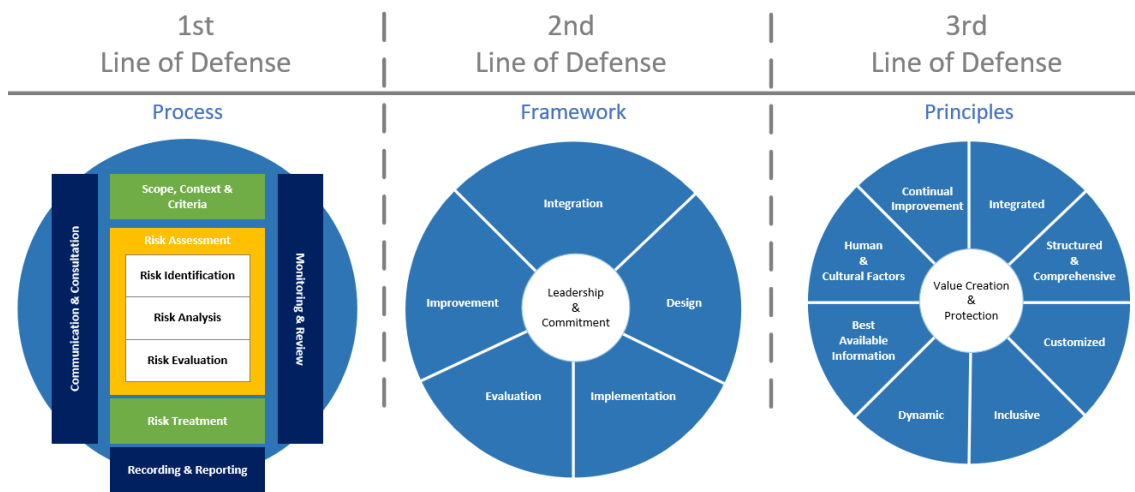


FIGURE 3. Risk management & the three lines of defense (ISO/IEC. 2018, cited 26.5.2018)

The first level of defense identifies the risk. After identification the risk management process analyses, evaluates and treats the risk. Second level of defense is responsible for setting up a framework which monitors that first the first level is handling risks properly. Second line of defense is also consistently trying to improve the framework and the design. Third level of defense applies principles to both first and second level of defense. In practice the third line of defense is internal auditing. (The Institute of Internal Auditors 2013, cited 23.3.2018.)

Incident response and business continuity are not directly part of risk management but they share a strong synergy with its functions. Despite all the measures and controls put in place, not all incidents can be prevented. When risk elimination is not possible the organization then moves into mitigating the effects of an incident. To address this, organizations are preparing plans and response procedures that handle these situations and ensure that the interruption will have minimal effects to operations. (Berman, 2015, cited 20.5.2018.)

2.2.1 Risk management as a process

After risk is identified the nature, source and type of impact for the risk have to be analyzed. This is achieved by creating a classification system for the risks. In risk classification the organization

identifies the types of risks which will enable the organization to understand the most vulnerable areas of its business. (AIRMIC, Alarm, IRM 2010, cited 2.4.2018.)

The development of risk appetite statement is the cornerstone of the organization risk management strategy. The risk appetite is the amount of risk an organization is willing to take. An appetite for risk is the formal way of expressing these risks. It is closely linked to the organization's business strategy. The risk appetite should be clearly defined and demonstrated within the tolerances and risk limits to ensure that the objectives of the organization can be achieved. (Pfetsch, Poppensieker, Schneider & Serova 2011, cited 6.4.2018.)

There is no unambiguous way to create the classification but the usual aspects are at least financial risks, operational risks, reputational risks and infrastructure risks. Financial control risks are the risks that are directly connected to money and therefore finance. Financial risks are not all risks that have financial impact and damage to organization. Financial risks are for example cash-flow and credit risks. Infrastructure risks are tightly related to organization's infrastructure, logistics and personnel. Organization's buildings and employees are prone to risks which when realized often lead to incidents. As the name suggests operational Risks are the risks directly connected to organizations operations. They can target organization's processes, supply chain, direct knowledge and know-how. Reputational risks are the risks that affect how the organization is seen by others. (AIRMIC, Alarm, IRM 2010, cited 2.4.2018.)

2.2.2 Framework

A number of standards have been created worldwide to support organizations in implementing methodical and efficient risk management. These standards are designed to provide a broad view of framework conditions, processes and practices and are generally defined by recognized international standards organizations or groups of companies. Risk management is a rapidly evolving discipline and standards are regularly updated and revised. The different standards reflect the different motivation and technical orientation of their developers and are suitable for different organizations and situations.

Standards are generally voluntary, although compliance with a standard by supervisory authorities or by contract may be required. Main purpose of these standards related to risk management is

allow organizations set up effective risk management framework (Institute of Risk Management 2018, cited 10.4.2018).

2.2.3 Principles & Internal Auditing

The organizations strategic objectives should be the basis for risk management. Therefore, Risk management's objectives should be to mitigate anything that will possibly compromise organization's mission statement. (Deutsche Bank 2016, cited 26.5.2018.).

Auditing is the party that enforces those principles. It monitors the effectiveness of the risk management system, particularly of the internal control system and the internal audit system so that the other lines of defense are operating as they should. (Deutsche Bank 2016, cited 26.5.2018.).

2.3 Compliance

Compliance is a process following and acting according to an order, rules or requests (International Compliance Association, cited 20.4.2018). Mastering the growing number of new regulations and laws and prioritizing regulatory compliance is a challenge. With the jungle of regulations, compliance has become more and more important for organizations. Companies have evolved over the course of time to comply with these regulations but they still have to reviewed and checked consistently. Without good compliance management, following these regulations will be impossible for international organization. Today, most of the industries have a tight set of rules and regulations which to play by (RSA 2017a, cited 24.3.2017). Even minor misdemeanors by large-scale enterprises can result in hefty fines which can be avoided if your compliance is in order. (EU GDPR Compliant 2018, cited 23.5.2018)

Latest example of the importance of compliance has been lately introduced in Europe. The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy (European Commission 2018, cited 25.5.2018).

2.3.1 Compliance Program

Compliance program is a collection of internal policies and procedures which helps organization to comply with laws and regulations. Similar to risk management also the importance of compliance programs has grown since the financial crisis. (Investopedia 2018b, Cited 2.4.2018.).

Well prepared compliance program can help organization in complying with all the procedures. Many of the laws and regulations are overlapping so well-set procedures may save organization's time as the same procedure complies to multiple laws and regulations. (RSA 2017b, Cited 2.6.2018.).

2.3.2 Reporting

In practice the compliance program's purpose is to support governance in its efforts to create more value to the business. One way to achieve this is by reporting the compliance issues. Compliance reporting can activate when a boundary is crossed or in order to prevent issues it can also launch when the boundary is neared. (Corlett Bolton & Co 2003. 24.3.2018.).

Reporting should be consistent throughout the organization and there should not be any exceptions. All operations and function should be bound report issues regardless their attachment to business strategy. (Corlett Bolton & Co 2003. 24.3.2018.).

3 REQUIREMENTS PLANNING

Requirements Planning is the first stage in the Rapid Application Design (RAD) Methodology lifecycle. Requirements planning should produce the organization a rough idea how its GRC processes work and how mature they are. From these steps the organization can then understand its requirements better and finalize the initial requirements for the system. As RAD principle is to involve end users in the project from the start, the organization should arrange a Joint Requirements Planning (JRP) workshop where everyone who is involved with the system participates. Requirements planning is divided into researching the current situation, defining requirements and finalizing requirements. (HKSAR 2009, cited 29.5.2018.). This chapter examines how to apply these principles in a GRC project.

3.1 Research current situation

When starting a research on the current situation, it is essential to understand the scope of the project and the current GRC maturity level. Organization should clearly define the current challenges it faces when dealing with GRC and what kind of requirements it has for new GRC tool. Organization has to ask from themselves where they we struggling and how can they solve it? (OCEG 2016, cited 24.3.2018.).

Many of the challenges and requirements can be traced from the maturity assessment as it should give the organization a clear understanding where they stand right now and where they want to be. For low maturity organizations simply implementing integrated GRC tool will solve many of the challenges and fill the requirements. (OCEG 2016, cited 24.3.2018.).

3.1.1 Program scope

To get started with the scope organization should start by defining the business processes related to GRC. Business processes give context for their surroundings. Based on business process-es the related assets can be deduced. Processes need to be supported with carefully prescribed roles, responsibilities and accountabilities. They also require an appropriate set of guiding principles and

organizational structures that fit the style, skills and operational norms specific to the enterprise. (SQA 2007, cited 31.5.2018.).

RAD uses Business Process Modelling (BPM) to understand current processes and their workflow. BPM does not only help in outlining the new system but it also can help in identifying issues and problems.



FIGURE 4. Simple process visualized in Business Process Modeling Notation (BPMN)

Business Process Modeling Notation (BPMN) is a standard way to display workflow and tasks. In the model events like start and end are marked with circles and actions are rectangular boxes. (Pearson 2018)

TABLE 1. Process description matrix

| Business Process | Description | Result |
|-------------------|-------------|--------|
| Business Process1 | | |
| Business Process2 | | |

Table contains the minimum requirements for defining the process. Process always consists of steps that eventually aim for a result (Veyrat 2015).

3.1.2 Maturity assessment

GRC maturity can be assessed with a maturity model. There is a wide number of GRC maturity models available from different vendors which are generally available for free. (Batenburg, Neppelenbroek & Shahim 2014.). The focus on this research is not invent a new maturity model but to explain how to use one. Maturity models are usually defined by using advancing stages or

levels which have a ranging numeric value. The maturity model should be chosen based on organization needs as some models can be more industry specific than others. For this research the chosen maturity model is OCEG Maturity Model for Integrated GRC which OCEG co-developed with RSA. (OCEG 2016, cited 24.3.2018.).



Figure 5. GRC maturity stages. (OCEG 2016, cited 24.3.2018).

The Figure 5 is displaying the different maturity stages for GRC. As figure shows the general trend of more mature GRC is moving from simply complying to finding opportunities with the help of GRC (OCEG 2016, CITED 24.3.2018).

GRC maturity should be assessed per each process. This will give the organization a very hands-on information on how well the function is performing. For example risk management can do well overall but the reporting function could be lacking. If simply assessing the entire risk management as a one function this will not be discovered. (Batenburg, Neppelenbroek & Shahim 2014.).

TABLE 2. Business process maturity matrix

| | Maturity Stage | | | | |
|---------------------------|----------------|----------------|-------------|---------------|----------------|
| Business process name | 1 – Siloed | 2 – Transition | 3 – Managed | 4 – Transform | 5 – Advantaged |
| Risk management: Process1 | | | | | |
| Risk management: Process2 | | | | | |

As it is visualized in the figure at the lowest maturity stage the organizations GRC functions are siloed, meaning that they are unaware of each other. This often means that organization has set

up some functions to support compliance requirements but the functions are still chaotic and ad hoc based. There is no knowledge transfer or integrations between different departments which is why collaborative reports and results cannot be achieved. Due to this and ad hoc based approach the methodology differentiates between different functions and processes. Organizations in this stage might not have an intention to strive for more mature GRC as the benefits are unknown for them. This means that GRC functions only aim satisfy must-have requirements in their own domain. This is the basic undeveloped stage for organization GRC. (OCEG 2016, cited 24.3.2018.).

When maturity grows in the GRC processes are getting more aware of each other. Yet, at transition stage they still might not exchange information or only certain processes exchange information but a real full cycle GRC integration is not established. Figure 5 describes the transform stage as the second lowest mature stage. In transition stage the organization's GRC is fragmented and even though the processes itself usually satisfy managements needs they do not provide an overview of the entire field and holistic understanding is not there. At this stage it is also very typical that one process is ahead of the others as organization is establishing common business hierarchy for reporting risk and compliance issues. These processes are leading the direction of company's GRC as benefits of using common practicalities and platform are starting to seem more obvious. This progress will eventually lead to building of common framework. As the name describes transition stage is a temporary stage where organization is building a more mature approach to GRC. In practice this means that organization already has or it is developing a GRC roadmap to achieve more mature GRC processes. (OCEG 2016, cited 24.3.2018.).

At the managed stage organization has established an integrated platform for GRC functions. Organization's GRC program is well underway and as seen in figure it has now moved into risk focused organization. This means that the organization is not just complying with laws and regulations but also actively managing and mitigating its risks. Organization is actively monitoring risks with the clearly defined first and second line of defense. This can be also seen in figure 5 as managed stage lines up with risk focused maturity. Organization is emphasizing this by arranging training and awareness campaigns targeting the staff dealing with processes. Role of the third level of defense is becoming more independent and it is now more clearly overseeing party as it will have a more holistic understanding due to integrated platform. Common methodology is established, functions are aware of each other and they are trading information with each other. Also the governance of GRC should by now formal. Organization can set up a committee for supervising and managing the GRC efforts. (OCEG 2016, cited 24.3.2018.).

The transform state focuses on aligning and improving the common functions established in integrated stage. As the same suggests and similar to transition stage the organization wants to achieve higher maturity. At this stage a clear change happens where organization is no longer just trying to manage risk but is also now starting to take into opportunities which are provided by GRC platform. Opportunity is a positive risk where organization stands to gain (usually financial) benefits for succeeding in it. In order to pave this way for taking opportunities the organization has to further bridge the gap between GRC processes and business. Opportunities can only be taken if the business is aware of such opportunities and this means getting them involved more actively into GRC. This means that the GRC projects are becoming increasingly harder and they require more commitment and supervision. Before aligned state, the board has only been interested in getting the reports out of GRC showing positive results but from now on the board has to figure how it can use GRC more effectively to support the business and decisions. (OCEG 2016, cited 24.3.2018.).

At the advantaged stage the organization has managed to optimize the business benefits of GRC and has mastered its risk management functions. Organizations that reach this stage do not only have a very well maintained GRC program but they also share a very strong passion to strive for the industry leading GRC. In this stage GRC can help out the organization to beat the competition and adjust itself better for harder times. Instead of acting on action, the organization can now predict outcomes and maybe even stop some disasters before they occur. However, at this point maintaining GRC can cost a lot of money. Before reaching this stage, most organizations have the mindset where maturing the GRC is only beneficial when it brings direct savings to GRC functions itself. The organizations who make it to optimized stage understand that GRC can increase the business value of functions even though it comes with a bigger price tag. (OCEG 2016, cited 24.3.2018.).

3.2 Define & Finalize requirements

After assessing all the functions belonging in the scope the organization could use the same assessment to picture where in the maturity model they would like to see the function in the near future. Most of the requirements should be already understandable from BPMN diagrams and related descriptions created earlier.

TABLE 3. Target maturity matrix

| Business process | Target maturity level | Requirements | Challenges |
|------------------|-----------------------|--------------|------------|
| | | | |

Requirements can be categorized as functional and non-functional requirements. Functional requirement describes a facility or feature required for the function. They should describe what the system should do or provide for users. Non-functional requirements describe the required functions and specific data details that is held in the system. Non-functional requirements focus on describing constraints, targets or control mechanisms that will be implemented in the new system. In essence they determine the quality of work that should be provided. (SQA 2007, cited 31.5.2018.).

4 USER DESIGN

In user design stage business activities and data are analyzed with a greater detail. At this stage organization has to create a plan on how to facilitate the existing functions to the new system. This requires mapping of applications and connecting them to each other. This requires drawing diagrams for each process to determine the workflow and to create high level design diagrams to understand how the applications are connected inside the solution. User design phase focuses on compiling all the data gathered in requirements planning and creating a one unified plan on how to implement the system. During this phase the procedures required for the functional system are identified. (HKSAR 2009, cited 29.5.2018.).

4.1 System Area Model & System design

System area model should paint the picture of how the system is connected from the inside. How each function relates to each other and in general what functions are included in the system. System design takes this one step deeper as it also wants to describe how the processes are completed in the system, initially giving the first idea of how to build the workflows in the system. In addition to this the first layouts should be designed here. (HKSAR 2009, cited 29.5.2018.). In RSA Archer this means describing the data visualization and data configuration elements that will be used in the system so that the development may begin.

In RAD model Joint Application Design (JAD) workshops are organized in order to bring system area model and system design quickly to satisfactory level. JAD workshops include tight collaborating between the users who will be using the system which effectively cuts the gap which is normally present between the users and the developers. JAD workshops can be held for the same individuals who were present during the JRP. The difference between JAD and JRP is that JAD goes deeper into detail in order to create a design that can be implemented as it is planned. (HKSAR 2009, cited 29.5.2018.).

During the JAD lots of initial implementation ideas are thrown around by the team. This method is called prototyping which is described as follows: "Prototyping is a technique for building a quick and rough version of a desired system or parts of that system. The prototype illustrates the system

to users and designers. It allows them to see flaws and so look for ways to improve the system." (HKSAR 2009, cited 29.5.2018).

Another technique used by RAD is cluster analysis which examines similar functions between different processes, entities and people. Analysis then helps to understand which processes are connected to each so that the bigger picture can be drawn. By understanding all the processes that belong under the same cluster a solution can be created. (HKSAR 2009, cited 29.5.2018.).

In RSA Archer this also helps the organization to understand how it can map its processes to existing RSA Archer applications.

4.1.1 Archer data visualization elements

RSA Archer's visual structure reminds folders and spreadsheets.

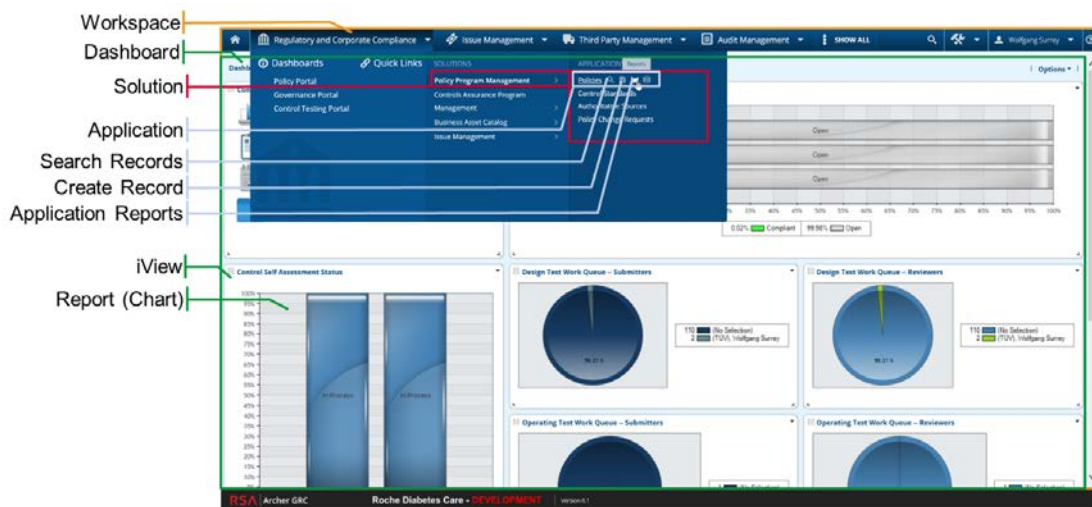


Figure 6. Typical RSA Archer end user landing page

As seen in the figure 6 Solution container is a grouping of related applications and questionnaires in RSA Archer that address a particular business need. Organization can arrange and create solution containers as they please because they are only a visual element which helps users understand better what they are dealing with. Workspace is a visual container that stores one or more dashboards and provides access to selected solutions and applications. Dashboard is then again, a container for one or more iViews. iViews can then for example contain reports and group related content. The power of this approach is to customize the layout for different roles and users

who access the system to enable them to make decisions, complete tasks, and stay up to date. (EMC Corporation 2013, cited 31.5.2018.).

Applications define the content and behavior of the individual records. It is a container for specific types of data records, such as incidents, controls, policies or assets. Applications are connected to each other with many-to-many relationships with no limitation to link. RSA Archer applications are divided into core-and on-demand applications. Core applications are cases pre-defined by and delivered with the RSA Archer standard installation and on-demand application are custom-built applications to support individual customer requirements. On-demand applications are not part of use-case licenses thus they always have to be licensed separately. (EMC Corporation 2013, cited 31.5.2018.).

Questionnaires are similar to applications. Difference between them is that the structure of questionnaires allows for assessing of specific application content. In order to create questionnaire, you always have to target an application. This makes questionnaire connections as many-to-one relationship to target application. (EMC Corporation 2013, cited 31.5.2018.).

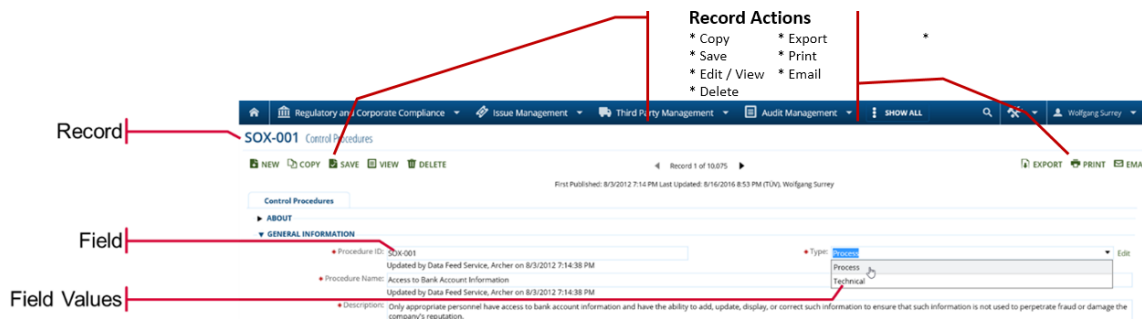


Figure 7. Record view

Record is an individual entry inside an application or questionnaire in RSA Archer. Records contain fields which the administrator can arrange to his liking inside the application builder. Field can be thought as a container which stores the specific data inside the record. There are different types of fields for different types of data and each field can be configured individually. For example, the can contain text, all kinds numerical data, values, calculations (which are linked related to formula builder). links to other fields, attachments and record permissions (which are related to access control). They can also contain record-based history log in Date/Time, User, Field and Action columns. (EMC Corporation 2013, cited 31.5.2018.).

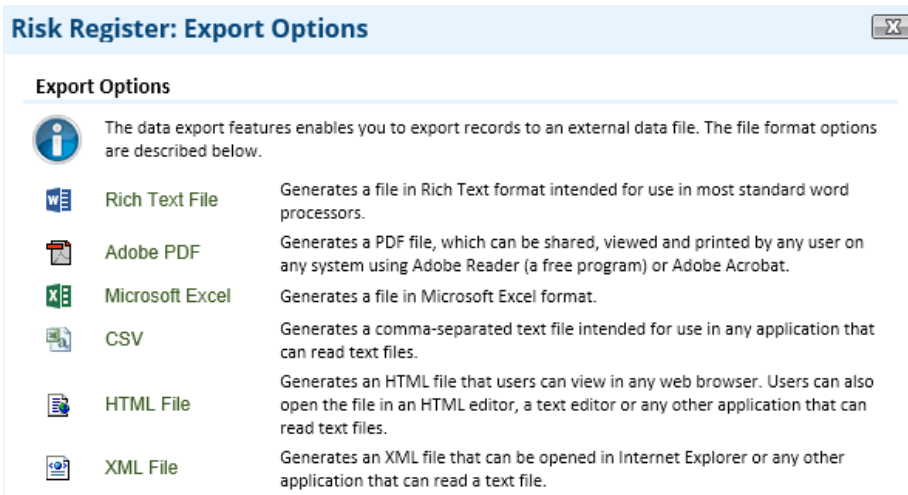


Figure 8. Archer report export options

In Archer, users can make a search of records by using filtering and sorting. These searches are then built into reports which can be saved for later use. Reports can be either saved for personal use or published globally which also enables using access rights features for reports. Archer enables users to create traditional row and column-based reports. Advanced reports can be built by applying sums, counts and grouping (to name a few) to chosen fields. Advanced reports can also be transformed into a graphical output giving horizontal and vertical graphs, pie charts and heatmaps. (EMC Corporation 2013, cited 31.5.2018.).

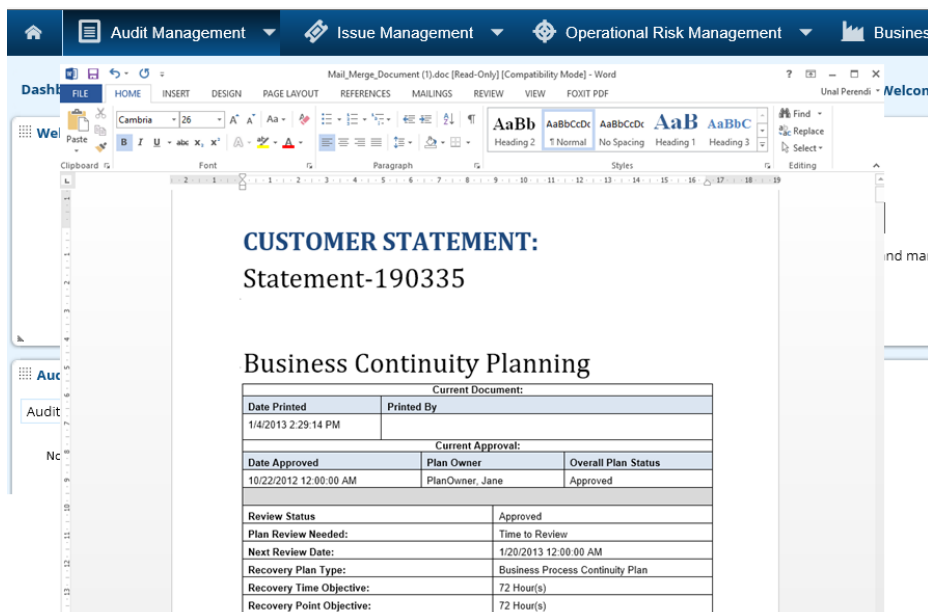


Figure 9. Example of a word document exported with mail merge function

Mail merge is a function that allows exporting of information to a pre-defined custom format. In RSA Archer a mail merge template can be uploaded to the platform and assigned to an application. Then when user exports data from the application an option to print it on mail merge template has appeared. As seen in the figure mail merge template could be for example a word document for a business continuity plan. (EMC Corporation 2013, cited 31.5.2018).

4.1.2 Archer data configuration elements

Platform developers have access to application builder. Modeling of data objects, like fields inside the applications and questionnaires is configured in application builder.

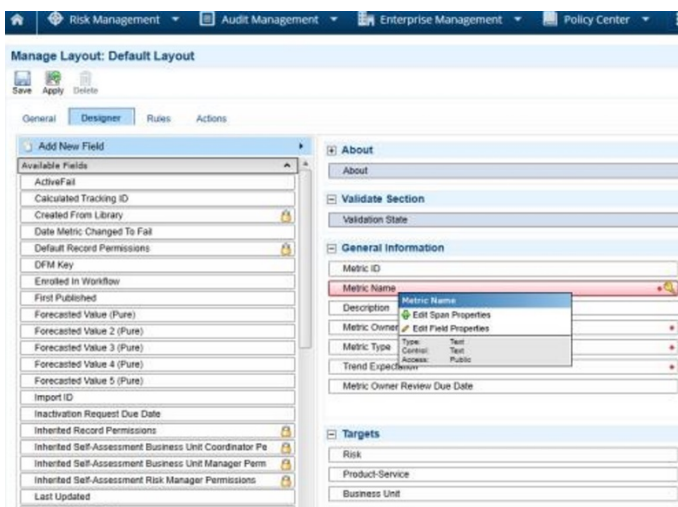


Figure 10. Application builder

Application builder is the place where platform developer will spend most of this time. By reaching the related field in the application builder, layout, conditioning, calculation and similar settings are set (EMC Corporation 2013, cited 31.5.2018).

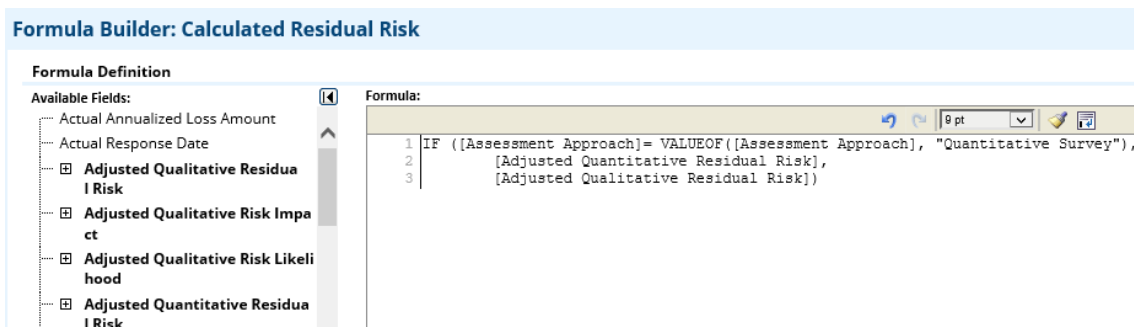


Figure 11. Formula builder

Formula builder assists the developer in creating calculations by giving a list of possible functions that can be used and giving links to other related field in the application and fields which are connected to an application with a cross-reference field. (EMC Corporation 2013, cited 31.5.2018.).

DDE (Data Driven Event) allows Archer to react dynamically for data conditions or values in the system. A DDE is a combination of a rule and linked actions. Rule is a set of conditions that must be evaluated as true. Rule order can be configured by the by the administrator. Data driven events are associated with individual layouts in an application or questionnaire. (EMC Corporation 2013, cited 31.5.2018.).

| Field To Evaluate | Operator | Value(s) |
|--|----------------|--------------------------------|
| 1. Response | Contains | No Selection Remediate Risk |
| 2. Criticality | Does Not Equal | High |
| Advanced Operator Logic: 1 OR 2 Example (1 AND 2) OR 3 | | |

Figure 12. DDE criteria

DDEs are configured to provide ability for dynamically controlled the page layouts based on the state of content, conditional filters or set field values based on the state of content or for example email notifications. An action is a predefined operation that is linked to a rule. Action is only executed if the conditions of the rule are evaluated as true. In above (Figure 12) example the action starts to show the whole section with making the Reviewer field read-only and Review Date as Required to enter based on the rule defined on the data. (EMC Corporation 2013, cited 31.5.2018.).

Archer also uses the same functional layout see in Figure 12 for enabling filtering and sorting in reports and fields. (EMC Corporation 2013, cited 31.5.2018.).

RSA Archer provides a variety of different notification types depending on the needs of the organization. Notifications enable recipients to receive notifications after the adding or updating of records in specified applications or questionnaires. Administrators can configure the default setups for notifications in notification blueprints. (EMC Corporation 2013, cited 31.5.2018.).

RSA Archer has 4 levels of access rights arrangements which provides flexibility to limit the access to the target information (EMC Corporation 2013, cited 31.5.2018.).

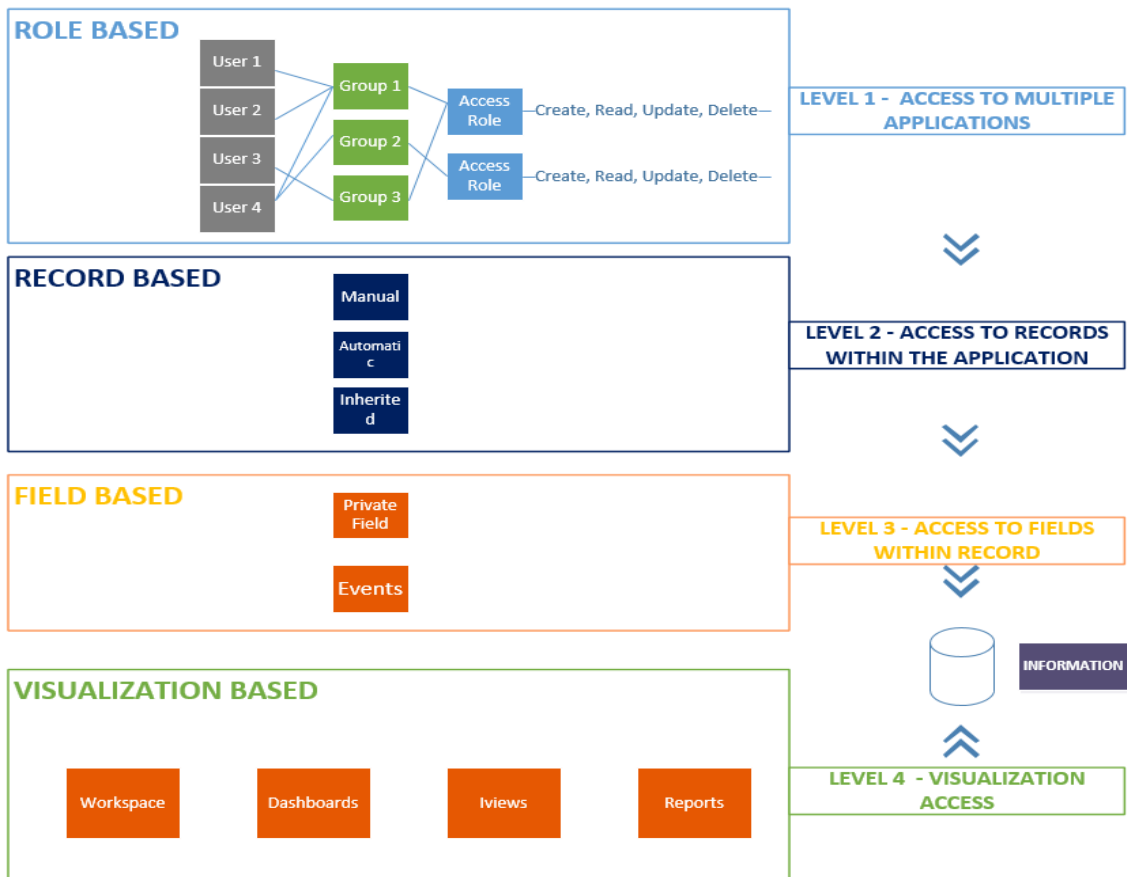


Figure 13. RSA Archer access control levels (Governify internal resources)

Access rights can be limited by typical roles and groups, by record permission fields which can grant access according to criteria, field-based restrictions which can hide only one field from record or with the visualization-based access rights where access is limited to containers and reports. (EMC Corporation 2013, cited 31.5.2018.).

Archer has numerous ways to extract, import & move data. Archer's ability to easily connect to external system and create integrations to other databases is one of the biggest selling points of the platform. It is possible to bring contacts and users from Microsoft Active Directory utilizing Archer's built-in LDAP Sync. One data feed that extracts information with an SQL query can bring organizations assets to Archer from other information libraries. For example, connection to HR-database can be established with one query. (EMC Corporation 2013, cited 31.5.2018.).

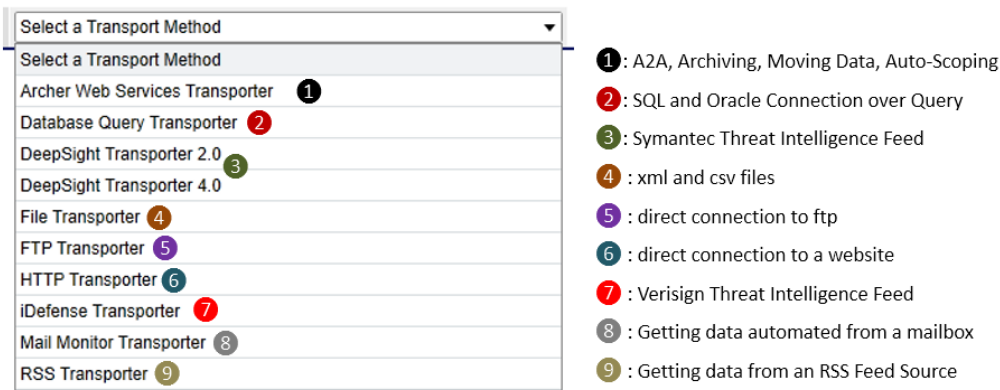


Figure 14. Different data feed transporters RSA Archer

The figure 14 only displays RSA Archer's capabilities with data feeds but there are also other ways to bring information to the platform like data importing which can be even executed by end user. Data imports are typically .csv files. After retrieving the queried table RSA Archer will let the user drag and drop data to map it to related fields. Data Imports are useful when it is required to do one-time data transition to Archer platform. (EMC Corporation 2013, cited 31.5.2018.).

Data feeds allow building of dynamic integrations with external enterprise systems and structured files (such as CSV, XML or DB View) that can run automatically on an on-going schedule (EMC Corporation 2013, cited 31.5.2018).

As confidentiality of the related records is important, in order to satisfy the segregation of duties, DB Administrators cannot find the records by querying the sql database. This also applies for integration to other systems (e.g.; BI Reporting tools). From exporting perspective, data publications are an easy method to publish the record content data to an SQL or Oracle Database Server. (EMC Corporation 2013, cited 31.5.2018.).

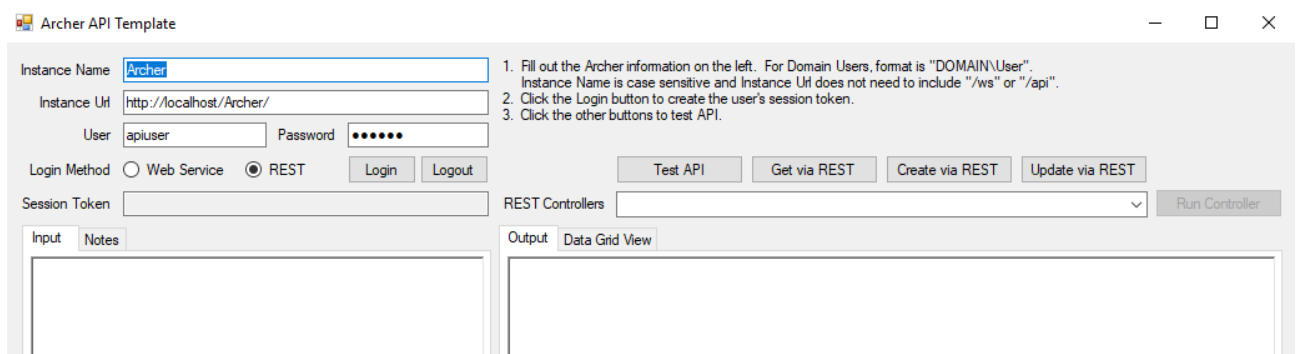


Figure 15. Archer API Template build for Visual C#.

As seen in figure 15 RSA Archer can also provide Web and REST API options for advanced development of integrations and other components. (EMC Corporation 2013, cited 31.5.2018.).

4.2 Prepare implementation strategies & refine system design

After building the first system design the organization can now keep refining and perfecting the design until it is ready. Refining the design takes less effort than the initial system design building. The final implementation plan should be based on system area model and system design created earlier. (HKSAR 2009, cited 29.5.2018.).

On top of this, the implementation strategies are applied which defines the schedule and implementation order of the project (HKSAR 2009, cited 29.5.2018.).

4.3 Finalize & Approve system design

System design finalization and approval is about accepting system area model and system design. During this step the organization confirms the plan for implementation according to implementation strategies. All the work that has been done so far culminates to this point where the design phase will be over and the system construction can begin. (HKSAR 2009, cited 29.5.2018.).

In order to start the development on RSA Archer platform an environment has to be configured.

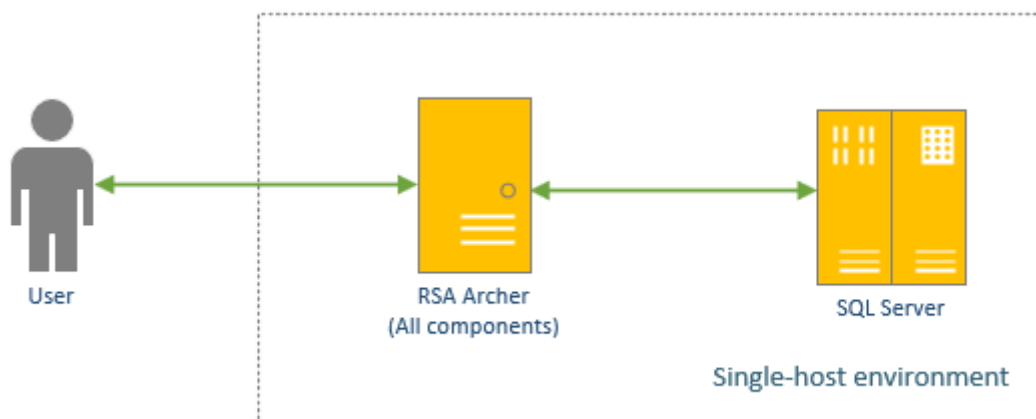


Figure 16. RSA Archer single-host environment architecture

Archer installations are described as either single-host environment or multi-host environment. The difference between the two is that in single-host instance all the Archer components are installed on the same server. Database is always recommended to be installed on a separate server. In multi-host environment web-application is installed on a separate server and the service components on another server. In practice this adds one more layer between the user and RSA Archer. Multi-host environment can support multiple web and services server. (EMC Corporation 2013, cited 31.5.2018.).

As RAD modeling promotes effective and descriptive documentation, it is important that organization evaluates all the diagrams, designs, models and plans so far so they can be used in the implementation (HKSAR 2008, cited 29.5.2018).

5 RAPID CONSTRUCTION

This chapter briefly describes how to install and setup RSA Archer and then explains the different key elements in it which can be used for the platform configuration. Different testing techniques are applied from RAD methodology.

In requirements planning and design phase the project was defined and eventually carved into system area plan and system design. Implementing RSA Archer requires platform installation, continuous platform configuration and testing. This also fits RAD as it aims for implementing and testing through iterations until the requirements are met. (HKSAR 2009, cited 29.5.2018.)

5.1 Preparing for rapid construction

In RAD methodology the preparation for rapid construction means preparing the environment for the development (HKSAR 2009, cited 29.5.2018). During task the RSA Archer is installed. Before installation it is important to a quick look at licensing as the license is applied during the installation. Licensing defines which use cases are available for the organization after the platform is installed. (EMC Corporation 2013, cited 31.5.2018.)

RSA Archer consists of 7 solution modules which each cover a number of solutions. These 7 solution modules then form use cases which are licensed to customer. Archer has 36 “out-of-box” use cases in total built on top of all solution areas (Appendix1). “Out-of-box” means that these use cases come ready with functionalities to use directly after license is bought. (RSA. 2018. cited 24.5.2018.). Use cases are delivered with “As is” principle meaning they are not tailored for customer. Building custom configurations to licensed use cases in order to meet organization's business requirements is free but it is customer's own responsibility.

RSA Archer Single-host installation process of RSA Archer platform is described in Appendix1.

5.2 System construction

As mentioned earlier RAD emphasizes using tools to automate and speed up the development (HKSAR 2009, cited 29.5.2018). This suits Archer very well because in many ways Archer works like an integrated CASE tool as the development is done by configuring elements. Archer incorporates tools to develop and configure the platform to suit individual organization needs. For example, organization can buy a use case and tailor it to suit its needs. (EMC Corporation 2013, cited 31.5.2018.). System design has been finalized and approved in user design phase and now it has to be implemented in an environment. All the documentation provided earlier can be used to assist this process.

5.3 Generating test data & system documents

In this task organization has to create a test plan for the system and generate system documents based on the developed environment. RSA Archer can be tested with the same general methods as the other software is tested. (HKSAR 2008, cited 29.5.2018.).

5.3.1 Test Plan & Data

A good method for creating a test plan is to use Five-fold Testing System which thinks of all the aspects that are related to testing (Kaner, Bach, Pettichord 2001, cited 31.5.2018).

"Testing follows a strict blueprint. This optimizes the use of - - skills, time, and money - - to take the product forward" (Bradford 2017, cited 31.5.2018).

Table 4. Five-fold testing technique described in matrix

| Dimension | What to ask? | Technique |
|-----------|---------------------------|--------------|
| Testers | Who is doing the testing? | User Testing |

| | | |
|---------------------------|---|--|
| Coverage | Which parts of the solution are tested? | Function testing, Requirements based testing |
| Potential Problems | What kind of issues is the test trying to find? | Input & Output constraints |
| Activities | What actions are performed? | Exploratory testing |
| Evaluation | What is the test passing criteria? | Self-verified |

The five dimensions are described in the table 4 with the question that enables the discovery of the dimension. Techniques chosen in the table 4 cover the development aspects of the RSA Archer environment.

User testing chooses the testing group to be the end users. This means that the testing plan is done generally keeping in mind this focus group. Due to this the coverage of test should be limited to aspects that the end users can test and they understand. Functional testing essentially tests all the functions of the system. To bring more structure to this requirements-based testing can be applied before this. Requirements-based testing limits testing coverage to requirements defined earlier in requirements planning. (Kaner, Bach, Pettichord 2001, cited 31.5.2018.)

Potential problems are discovered from input and output constraints. For example, in RSA Archer it could mean checking if a field works correctly. If field should only accept numeric values and text can be entered a flaw has been discovered. For output constraints this would mean checking if a calculated field returns the correct value. (Kaner, Bach, Pettichord 2001, cited 31.5.2018.)

As mentioned before, RAD model encourages strong user presence throughout the project. (HKSAR 2009). Therefore, exploratory testing can be used as an test activity. There is no need to build testing scenarios as the users should already understand the basics of the system as they have been familiar with the processes before and they have been designing how they should be implemented in the system. Also due to this evaluation can be self-verified. This means that users can check and understand themselves if the was passed or not (Kaner, Bach, Pettichord 2001, cited 31.5.2018).

After the plan is created it is important to create some test data to the system so that the test plan can be conducted later.

5.3.2 Manuals & Technical Documentation

There should be separate system documents for separate roles in the system. Organization has to decide how it will handle creating different documents for administrators, end users & IT which will maintain the system. (HKSAR 2008, cited 29.5.2018.).

In addition to this a final technical system documentation should be created. This document should be combined from previous efforts on diagrams and system design documents. This document should also contain the necessary system architecture information.

5.4 Preparing for transition

In RAD all the required tasks for transition are carefully planned before executing them. After entering the transition phase, the project will not return to rapid construction phase as the transition phase focuses on ending the project successfully. (HKSAR 2009, cited 29.5.2018.).

In preparing for transition organization creates plans on how it will import existing information in the new system and how it will train its staff. Additionally, the organization has to choose how it will deploy the new system in production. (HKSAR 2018, cited 29.5.2018.).

5.4.1 Data Conversion

When preparing for transitioning from one system to another a data conversion from old system to a new one has to be performed. Also, possible other integrations have to be performed. RSA Archer's data feed feature and LDAP configuration offers tools for migrating data. (EMC Corporation 2013, cited 31.5.2018.).

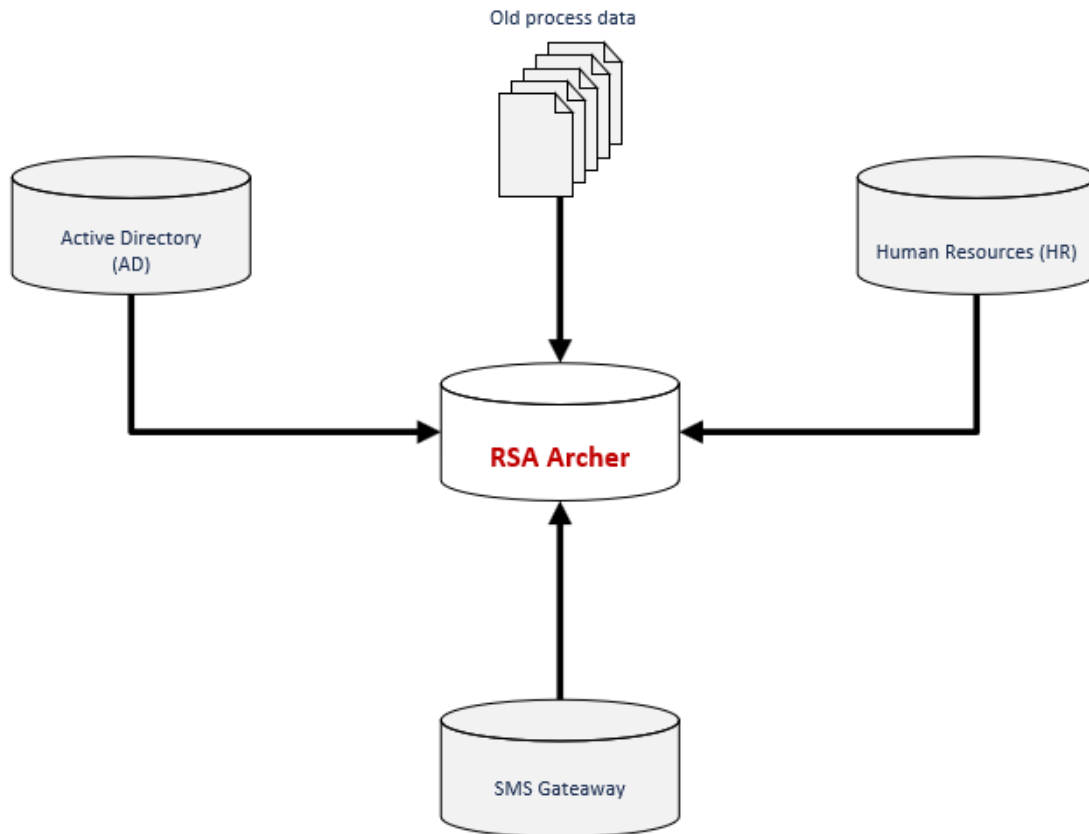


Figure 17. Example diagram describing data importing sources for RSA Archer

As seen in figure 17 RSA Archer can receive information from multiple sources and in different ways. Based on this organization can plan how it will import all the existing data to RSA Archer. (EMC Corporation 2013, cited 31.5.2018.).

5.4.2 Packaging

Archer features a possibility to create packages of existing system functions. What this means is that the organization can package the solution created in development environment and deploy it to production. (EMC Corporation 2013, cited 31.5.2018.).

| Packages ⓘ | |
|--------------|----------------------|
| Name | Status |
| Issues | Successful |
| Test Package | Partially Successful |
| issues | Not Generated |

Figure 18. Created packages

Packages can be created from use case application and custom application. It is important to understand that the environment where the package will be taken should have the equal license to where it was packaged.

5.4.3 Training plan

An effective training requires organization to train all groups involved with the software. In RSA Archer this mainly means the administrators, end users and IT-team (MSH 2012, cited 1.6.2018). Similar to testing it is important to create a training methodology that can be used to create training plans for different groups.

In order to create a successful training, the organization has to set up goals for the training. Goal is to get end users quickly to the level where they are comfortable using the system and they can complete the processes they have already done before implementing the system. To do this effectively the organization has to take into account that end user skillsets are on different levels. Some individuals will progress faster than others and due to this it is also important to deliver the information in multiple ways. Besides giving users a training manual, face-to-face to training sessions can be conducted. For example, the end user training should not focus on how to use RSA Archer but on how to execute organization's own processes on RSA Archer. Because the training is focused on organization's processes it will bring benefit to create own training program for the organization. This way the training can also be scaled in the future if more users will start using the platform. (The SunView Team. 2013.)

5.5 Verifying system construction

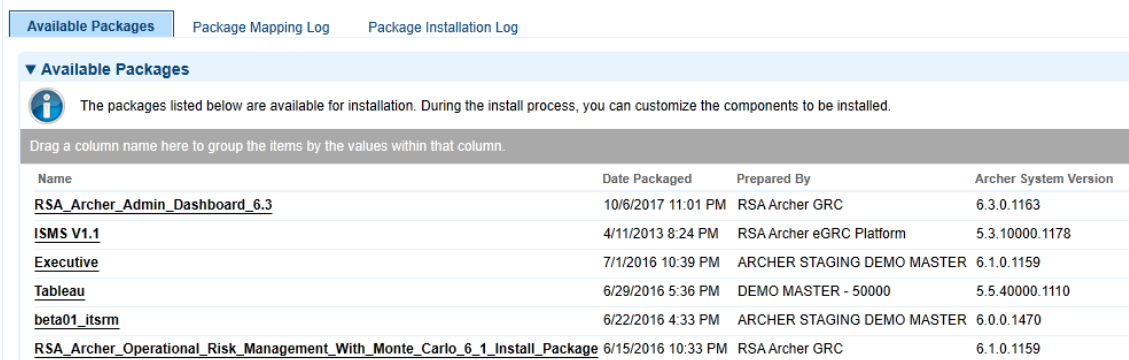
After tasks are completed in rapid construction the phase should be fully verified. As this is the last step before transitioning the new system into production it is paramount to make sure everything works as intended. Essentially, in this phase the organization will authorize the new system. (HKSAR 2009, cited 29.5.2018.).

In order to this organization has to execute the test plan created earlier. If the system passes all tests then it can be deployed to production. If the system does not pass the tests or if other

development iterations are planned the project should not proceed to transition. (HKSAR 2018, cited 29.5.2018.).

6 TRANSITION

The transition is the final phase of RAD model. During this phase the new system will replace the old one. To achieve this the data and connections have to be arranged from old system to a new one and if new arrangements are made like integration to Active Directory (which might not have been possible before) they should be activated and tested to be functional. (HKSAR 2018, cited 29.5.2018.).



| Name | Date Packaged | Prepared By | Archer System Version |
|---|--------------------|----------------------------|-----------------------|
| RSA_Archer_Admin_Dashboard_6.3 | 10/6/2017 11:01 PM | RSA Archer GRC | 6.3.0.1163 |
| ISMS V1.1 | 4/11/2013 8:24 PM | RSA Archer eGRC Platform | 5.3.10000.1178 |
| Executive | 7/1/2016 10:39 PM | ARCHER STAGING DEMO MASTER | 6.1.0.1159 |
| Tableau | 6/29/2016 5:36 PM | DEMO MASTER - 50000 | 5.5.40000.1110 |
| beta01_itsrm | 6/22/2016 4:33 PM | ARCHER STAGING DEMO MASTER | 6.0.0.1470 |
| RSA_Archer_Operational_Risk_Management_With_Monte_Carlo_6_1_Install_Package | 6/15/2016 10:33 PM | RSA Archer GRC | 6.1.0.1159 |

Figure 19. Packages ready to be installed

Also, the developed system has to be brought to production. In RSA Archer there are multiple ways to accomplish this. Seen in the Figure 19 is RSA Archer where packages from another RSA Archer environment are ready to be executed. This is one way of bringing clean installation to production after development. Another way to bring RSA Archer instance from development to production is to copy the database and re-install Archer on production environment. Third option is to promote the development environment to production environment.

During the transition all the plans created in preparing for transition should be performed. Training program which was planned in preparing for transition should be started. Transition is considered to be done once the organization approves the new system design which is now in production. (HKSAR 2009, cited 29.5.2018.).

7 CONCLUSION

Topics related around GRC are bound to be broad. It combines three massive topics under one umbrella which is then even harder to explain. Luckily, GRC was not invented so it would be easier to explain but rather because the components share a strong synergy and they are always interrelated one way or another. None of these components can perform to their fullest without the others. This is also why the magnitude of GRC is not really understandable when the person first comes across the GRC term.

One hour of good planning can save a full day's work in implementation. Having a clear and repeatable structure helps in forming habits and processes which can later help the process evolve even better. This is true for all GRC, project planning and software deployment alike. RAD fits well for projects with a clear end. RAD does not have real planning phase as instead of that it is going straight to requirements and creating the design. Also, RAD would not be suitable for GRC program as it does not have continuity or change management after transition.

The most distinguishable feature of RSA Archer Platform is that it is a complete, full-stack GRC solution for large organization. All the solutions for GRC can be found under one big business application which comes with few benefits and concerns. Full scale Archer solution is not suited for smaller or even most medium sized companies as it will be an overkill.

When doing research on GRC one is required to have some media literacy skills in filtering what is actual information and what is just vendor talk. GRC field is extremely biased due to lack of open sources and most available resources being guides and brochures written by different vendors. However, one common thing among these resources is that they all praise a well implemented integrated GRC solution. After doing the research and understanding how fragmented the information is, it is easy to agree with them. It was at the same time interesting and also a little bit frustrating to admit that every time when one topic got a closure at least two new topics opened. On the other hand, that also strengthened my belief that having a basic framework focusing very much on practical execution could serve a purpose in the field.

Despite the challenges faced I think that the outcomes of the research are only positive. Examining the topic has given me a broader view on GRC and has therefore made me feel more proficient in the work I do on daily basis. Besides all this, I also hope this will raise interest in the readers towards GRC. Working with GRC and different projects.

REFERENCES

Scottish Qualification Authority (SQA). 2007. Perform Structured Systems Analysis

Cited 31.5.2018

https://www.sqa.org.uk/e-learning/SDM03CD/page_02.htm

RSA. 2018. RSA Archer Solutions & Use Cases

Cited 24.5.2018

<https://community.rsa.com/docs/DOC-40093>

EMC Corporation. 2013. RSA Archer GRC Platform 5.3 SP1 Administrative Guide

Cited 31.5.2018

https://community.rsa.com/servlet/JiveServlet/downloadBody/14888-102-3-3702/GRCPlatform_5.3SP1_AdministratorGuide.pdf

Batenburg, R, Neppelenbroek, M, Shahim, A. 2014. A maturity model for governance, risk management and compliance in hospitals

Cited 24.3.2018

<http://www.sciedupress.com/journal/index.php/jha/article/viewFile/3283/2464>

OCEG. 2016. A Maturity Model for Integrated GRC

Cited 24.3.2018

<https://go.ocerg.org/maturity-model-integrated-grc#action>

Deutsche Bank. 2016. Risk Report

Cited 26.5.2018

https://annualreport.deutsche-bank.com/2016/ar/servicepages/downloads/files/dbfy2016_risk_report.pdf

Veyrat, P. 2015. Business process modeling examples

Cited 25.5.2018

<https://www.heflo.com/blog/process-modeling/business-process-modeling-examples/>

Pearson, S. 2018. 9 Best Business Process Modeling Techniques (With Examples)

Cited 1.6.2018

<https://tallyfy.com/business-process-modeling-techniques/>

Management Sciences for Health (MSH). 2012. Chapter 52: Designing and implementing training programs

Cited 1.6.2018

<https://www.msh.org/sites/msh.org/files/mds3-ch52-training-mar2012.pdf>

Kaner, C, Bach, J, Pettichord, B. 2001. LESSONS LEARNED IN SOFTWARE TESTING

Cited 31.5.2018

http://www.testingeducation.org/BBST/testdesign/KanerBachPettichord_Lessons_Learned_in_SW_testingCh3-1.pdf

The SunView Team. 2013. 5 Keys to Developing an End User Training Plan

Cited 1.6.2018

<https://www.sunviewsoftware.com/blog/learn/blog/5-keys-to-end-user-training>

The Government of the Hong Kong Special Administrative Region (HKSAR). 2009. An Introduction to Rapid Application Development (RAD)

Cited 29.5.2018

https://www.ogcio.gov.hk/sc/our_work/infrastructure/methodology/system_development/past_documents/rad/doc/g47a_pub.pdf

The Government of the Hong Kong Special Administrative Region (HKSAR). 2018. RAD Procedures Guide

Cited 29.5.2018

https://www.ogcio.gov.hk/en/our_work/infrastructure/methodology/system_development/past_documents/rad/procedures_guide.html

The Government of the Hong Kong Special Administrative Region (HKSAR). 2008. Summary of deliverables to be produced in each stage

Cited 29.5.2018

https://www.ogcio.gov.hk/en/our_work/infrastructure/methodology/system_development/past_documents/rad/doc/rad_delitask.pdf

Bradford, L. 2017. Everything You Need to Know About Software Testing Methods

Cited 31.5.2018

<https://www.thebalancecareers.com/all-you-need-to-know-about-software-testing-methods-4019921>

Gelnaw, A, Marden, M. 2017. The Business Value of RSA Archer in Making Governance, Risk, and Compliance Operations More Effective and Efficient

Cited 2.4.2018

<https://www.rsa.com/content/dam/pdfs/2-2017/idc-businessvalue-rsaarcher.pdf>

OCEG, What is GRC

Cited 17.3.2018

<https://go.oceg.org/what-is-grc>

Sheng, Y. 2009. What is Good Governance?

Cited 16.5.2018.

<https://www.unescap.org/sites/default/files/good-governance.pdf>

Investopedia. 2018a. What is Corporate Governance

Cited 2.4.2018

<https://www.investopedia.com/terms/c/corporategovernance.asp>

Investopedia. 2018b. Compliance program

Cited 2.4.2018

<https://www.investopedia.com/terms/c/compliance-program.asp>

Hernaus, T. 2008. Process-based Organization Design Model: Theoretical Review and Model Conceptualization

Cited 23.3.2018

<https://hrcak.srce.hr/file/201935>

PwC. 2016. Enterprise Risk Management—Aligning Risk with Strategy and Performance

Cited 24.4.2018

<https://www.coso.org/Documents/COSO-ERM-draft-Post-Exposure-Version.pdf>

IT Governance Institute. 2006. IT Control Objectives for Sarbanes-Oxley

Cited 23.3.2018

<https://ht.transparencytoolkit.org/FileServer/FileServer/clienti/Clever%20Consulting/standards/SOX%20and%20IT%202nd%20edition.pdf>

AIRMIC, Alarm, IRM. 2010. A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000

Cited 2.4.2018

https://www.theirm.org/media/886062/ISO3100_doc.pdf

Corlett Bolton & Co. 2003. Good Governance, Risk Management and Compliance (“GRC”) - Running the modern company

Cited 23.3.2018

<http://www.corlettbolton.com/assets/Uploads/Good-Corporate-Governance-GRC.pdf>

ISO/IEC. 2009. IEC/ISO 31010 Risk Management – Risk Management Techniques. Geneva: IEC

ISO/IEC. 2018. Risk management — Guidelines

Cited 26.5.2018

<https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en>

Bird, K. 2009. New ISO standard for effective management of risk

Cited 20.4.2018

<https://www.iso.org/news/2009/11/Ref1266.html>

The Institute of Internal Auditors. 2013. IIA Position Paper: The Three Lines of Defense Ineffective Risk Management and Control

Cited 23.3.2018

<https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf>

Berman, A. 2015. Risk Management and Business Continuity: Improving Business Resiliency
Cited 20.5.2018

<http://www.riskmanagementmonitor.com/risk-management-and-business-continuity-improving-business-resiliency/>

Pfetsch, S, Poppensieker, T, Schneider, S & Serova, D. 2011. Mastering ICAAP: Achieving excellence in the new world of scarce capital.

Cited 6.4.2018

<https://www.mckinsey.com/~media/McKinsey/Business%20Functions/Risk/Our%20Insights/Mastering%20ICAAP/Mastering%20ICAAP.ashx>

Institute of Risk Management. 2018. About Risk Management

Cited 10.4.2018

<https://www.theirm.org/the-risk-profession/risk-management.aspx>

International Compliance Association. What is compliance?

Cited 20.4.2018

<https://www.int-comp.org/careers/a-career-in-compliance/what-is-compliance/>

EU GDPR Compliant. 2018. Fines for non-compliance

Cited 23.5.2018

<https://eugdprcompliant.com/fines-for-non-compliance/>

European Commission. 2018. A new era for data protection in the EU

Cited 25.5.2018

https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf

RSA. 2017a. RSA Archer Regulatory & Corporate Compliance Management

Cited 24.3.2018

<https://www.rsa.com/content/dam/en/solution-brief/rsa-archer-reg-corp-compliance-mgmt.pdf>

RSA. 2017b. Maturity Model Snapshot: RSA Archer Regulatory & Corporate Compliance Management

Cited 2.6.2018

<https://www.rsa.com/content/dam/en/maturity-model/regulatory-and-corporate-compliance-management-extended.pdf>

RSA Security LLC, 2018a. RSA Archer GRC Platform

Cited 24.3.2018

<https://www.rsa.com/content/dam/en/data-sheet/rsa-archer-grc-platform.pdf>

RSA Security LLC, 2018b. Governance, Risk & Compliance

Cited 24.3.2018

<https://www.rsa.com/en-us/products/governance-risk-and-compliance>

Gimon, Z. Understanding the rapid application development model

cited 31.5.2018

<https://theappsolutions.com/blog/development/rad-model/>

1. Installation Readiness Information Gathering Form must be filled.
2. License key must be available in case of unseen circumstances.
3. Check the environment architecture to determine server roles (web server, services server etc.)
4. Check the availability of the accounts for the servers
5. Check if Archer will be run on Local System or Domain Account
6. Login to server to make sure credentials are working properly.
7. Check that you have the required installation files for DB Server if DB Server installation is required:
 - a SQL Server Installer
 - b SQL Server Management Studio (SSMS)
8. Check that you have the required installation files for all other servers:
 - a Archer GRC Platform Installer (6.x)
 - b Filter Pack (2.0) Installer
 - c Java Runtime Environment Installer (8.x)
 - d .NET Framework (4.6.1) Installer
 - e Silverlight (5.5)
9. Hardware/server configuration should be checked that it matches the information given in installation Readiness Information Gathering form
10. Ensure no special process will be running during the installation, such as, Windows Backup, DB backup, Data Publications, UCF activity.
11. Check that Archer needed ports are open, e.g. SMB ports and AWF.
12. Check hostname and FQDN of the server.
13. Contacts from Windows, DB, Network, Archer Application Team, Vendor (phone and emails)

Installing the Components. Run this installation on your Server to install RSA Archer.

1. Install .NET framework. Minimum version 4.6.1
2. Run SQL Server Installer
3. Enter SQL Server License
4. Select the required features for installation and continue
 - a. Select atleast the following features:
 - i. Instance Features

- ii. Database Engine Services
 - 1. SQL Server Replication
 - 2. Full-Text and Semantic Extractions for Search
 - 3. Data Quality Services
 - iii. Shared Features
 - 1. Data Quality Client
 - 2. Client Tools Connectivity
 - 3. Integration Services
- 5. Name the SQL Server Instance and continue
- 6. Ensure on Collation Tab that Database engine collation is SQL_Latin1_General_CP1_CI_AS and continue
- 7. On Server Configuration select Windows Authentication mode and add current admin account as SQL Server Admin. Complete the installation
- 8. Launch SSMS Installer
- 9. Complete the installation and restart the server
- 10. Login to SSMS using your preferred login method
- 11. Right-click Server name, open properties and go to advanced and Max degree of Parallelism to 1
- 12. Create and configure configuration database
 - a. Create new database for configuration database.
 - b. Collation should be set SQL_Latin1_General_CP1_CI_AS
 - c. Autogrowth settings should be set to increase by MB not by %. Set to 64MB
 - d. Ensure log datafile has a size limit
 - e. Set Recovery Model to Simple and make sure Collation is SQL_Latin1_General_CP1_CI_AS
 - f. Give it a meaningful name like config_database unless client suggests otherwise
- 13. Create and configure instance database
 - a. Create new database for configuration database.
 - b. Collation should be set SQL_Latin1_General_CP1_CI_AS
 - c. Autogrowth settings should be set to increase by MB not by %. Set to 64MB
 - d. Ensure log datafile has a size limit
 - e. Set Recovery Model to Simple and make sure Collation is SQL_Latin1_General_CP1_CI_AS
 - f. Governify naming method is year+order number. For example 2018001
- 14. Create a new login to use as db owner. Choose name and password and press OK
- 15. Go back and assign db_owner role for instance and configure db
- 16. Check Server Locale
- 17. Install .NET framework. Minimum version 4.6.1
- 18. Install latest MS Filter Pack is installed.
- 19. Install JRE 8
- 20. Restart the server
- 21. Open Add roles and Features Wizard Install IIS server role and other features
- 22. Proceed and choose Server roles
 - a. From Server roles choose:
 - i. IIS
- 23. Choose the recommended features required for Archer installation and proceed
 - a. From Features choose:

- i. .NET Framework 4.5
 - ii. ASP.NET 4.5
 - iii. HTTP Activation
 - iv. TCP Port Sharing
 - v. Telnet Client
- 24. Choose the recommended Web Server Role Services for Archer and proceed
 - a. From Web Server Role Services Choose:
 - i. Default Document
 - ii. Directory Browsing
 - iii. HTTP Errors
 - iv. Static Content
 - v. HTTP Redirection
 - vi. HTTP Logging
 - vii. Static Content Compression
 - viii. Dynamic Content Compression
 - ix. Request Filtering
 - x. Windows Authentication (if sso is used)
 - xi. Net extensibility 4.5
 - xii. ASP.NET 4.5
 - xiii. ISAPI Extensions
 - xiv. ISAPI Filters
 - xv. IIS Management Console
- 25. Open IIS Manager and Expand Webserver options
- 26. Right-click Application Pools and create a new one. Give it a meaningful name like ArcherAppPool
- 27. Open Application Pool you created, go to Advanced Settings and
 - a. Change the Identity to user that will run archer
 - b. Check that .NET CLR Version is v4.0
- 28. Create the folder structure in root for Archer and ensure Archer Service account has full access to these folders
 - a. ArcherFiles
 - i. Logging
 - ii. 2018001 (Instance name)
 - 1. DataFeed
 - 2. Index
 - 3. Repository
- 29. Extract Archer Installer package and launch ArcherInstall as Administrator
- 30. Choose to Install all components and press next
- 31. Choose to create a new X.509 Certificate and press next
- 32. Define Configuration database for installation and use the login created earlier and continue
- 33. Skip Advanced Workflow HTTPS configuration and press next
- 34. Select platform language. This should be equal to System Locale
- 35. Define Instance database for installation and use the login created earlier and continue
- 36. Choose the same timezone as server is using and continue
- 37. Configure the IIS Settings for Archer
 - a. Website: Default Website

- b. Install in an IIS Application pool. Choose create new and assign it to ArcherAppPool you created earlier. Do not change application name
- 38. Choose to install only HTTP configuration
- 39. Choose not to use Instrumentation Service and press next
- 40. Choose the account to run Archer Services and press next
- 41. Choose to install Archer Program Group for all users and continue
- 42. Choose not to configure RSA Caching Service
- 43. Assigning the installation logging to the higher level Install logs folder you created earlier and press next
- 44. Finish the installation and restart server
- 45. Open Archer Control Panel and configure General Installation Settings
 - a. Set logging path to folder you created earlier
 - b. Change locale to United States (English).
 - c. Sync time zone with Server Setting
 - d. Save
- 46. Stay in ACP and choose Add New Instance and name it as you named Instance database
- 47. Configure Instance General settings
 - a. Set Instance use as Production
 - b. Change File Repository path to folder you created earlier
C:\ArcherFiles\2018001\Repository\
 - c. Change Search Index path to folder you created earlier
C:\ArcherFiles\2018001\Index\
 - d. Set this server as your Queuing Server
 - e. Set Notification Server Address.
 - f. Set Default from Address In case missing fill bogus@eaa.com so you can proceed
- 48. Define Instance Web Settings
 - a. Base URL: http://client.domain.com/RSAarcher
 - b. Authentication : /default.aspx
- 49. Define Instance Database Settings
 - a. SQL Server: Choose the one where you created databases
 - b. Login name and password: Use the login you created for server
 - c. Database: Instance database name
- 50. Define Instance Data Feed Settings
 - a. Enable access to Data Feed Manager for this instance
 - b. Set Data Feed Home directory to one you created before
- 51. Define SSO instance Settings
- 52. Define Instance Accounts Settings
- 53. Save Instance & Enter License Information
- 54. Save Instance again

Post Installation tasks

Run this installation on each services and cache server.

1. Go to ACP and Rebuild Search index

2. Go to webconfig and configure HTTPS and SSO
3. Go to IIS Manager and Create HTTP Redirection from Default website to Archer login page
4. Sync server time with ACP time zone and current.
5. Ensure installation account and service account used by Archer have access rights for folders under IIS App Pool
6. Check that search indexes and RSA Archer Queuing services are running on the same services server.
7. Create a test record
8. Check that AWF is working
9. Check that SSO is working if used
10. Run Monitoring console in ACP and check roles
11. Run Configuration and Installation report from ACP
12. Back up the instance and configuration databases
13. If no maintenance jobs are set archer default plan
14. Ensure that CPU/RAM/Disk figures are not critical