POLITECNICO
MILANO 1863

SCUOLA DI INGEGNERIA INDUSTRIALE
E DELL'INFORMAZIONE

Implementation of a GRC tool within an Italian company

TESI DI LAUREA MAGISTRALE IN
COMPUTER SCIENCE AND ENGINEERING
INGEGNERIA INFORMATICA

Author: **Andrea Galazzini**

Student ID: 903453
Advisor: Stefano Zanero
Co-advisor: Désirée Gnesini
Academic Year: 2021-22

Abstract

This thesis describes the experience of implementing a Governance, Risk and Compliance system, with particular attention to Information Technology Risk Management components, in a medium-sized multinational insurance company.

The adopted GRC software was Archer. Thanks to this choice, the project revolved around the configuration of the platform while the effort of developing new software has been minimal.

The thesis focuses the attention on the activities carried out by the author as an intern at the consulting company that supported the work.

Key-words: Governance Risk and Compliance, IT risk management, Archer, cybersecurity, risk-based, insurance company.

Abstract in italiano

Questa tesi descrive l'esperienza di implementazione di un sistema di Governance, Risk e Compliance, con particolare attenzione alle componenti di Information Technology Risk Management, in una multinazionale assicurativa di medie dimensioni.

Il software GRC adottato è Archer. Grazie a questa scelta, il progetto ha ruotato attorno alla configurazione della piattaforma mentre lo sforzo di sviluppo di nuovo software è stato minimo.

La tesi focalizza l'attenzione sulle attività svolte dall'autore come stagista presso la società di consulenza che ha supportato il lavoro.

Parole chiave: Governance Risk and Compliance, Gestione del Rischio Informatico, Archer, sicurezza informatica, risk-based, compagnia di assicurazioni.

Contents

1 Introduction

In recent years, the increasing dependence on technology has led to an exponential growth of the digital world. The rise of the Internet and the widespread use of digital devices have made it easier for individuals and organizations to store, share and access information. While this has brought many benefits, it has also made it more vulnerable to cyber-attacks. Cybersecurity is a critical concern for both individuals and organizations alike and is becoming increasingly important as the volume of digital data continues to grow. For this reason, it is important, for organizations, to adopt GRC management solutions.

"GRC (Governance, Risk, and Compliance) Management is defined as the automation of the management, measurement, remediation and reporting of controls and risks against objectives, in accordance with rules, regulations, standards, policies and business decisions" [1].

Like any other complex business automation activity, GRC requires the adoption of appropriate IT tools and a project for their implementation.

Various GRC tools are available today on the market, keeping the companies from developing their own custom software. Some of these tools are extremely flexible and configurable, managing to adapt to very different business realities, without having to modify the software code, and thus allowing for easier and safer maintenance of the instrument.

Nevertheless, although GRC tools being extremely powerful and configurable, the process of their implementation can be very complex as well as long to see through. The complexity of the process usually depends less on the complexity of the tool, than on the GRC involving nearly all business areas and a very large number of users: no business area can be said to be risk-free nowadays, especially in terms of cyber security. In addition, since all business users must be aware of the threats and how to deal with them, training is expensive and takes a long time to complete.

This thesis describes the implementation project of a GRC, in a medium-sized company of the insurance sector, and, in particular, the activities that I personally carried out, as an intern. The project is still in progress, although many important milestones were already successfully accomplished.

In particular, I will focus on the development of the IT risk domain, a fundamental part of the GRC, which saw me particularly involved in the definition and implementation of the solution, as it was the right training ground to introduce me to the job, according to my studies.

My involvement in the project was due to my role as an intern of HSPI S.p.A.

HSPI [2] is a management consulting company that has been active for 20 years, supporting its clients through the processes of change generated by Information & Communication Technology. HSPI uses an operational model capable of integrating distinctive management consulting skills and specialized knowledge in the ICT field.

HSPI has over 180 professionals, including managers, experts, and young talents and an annual turnover of 22 million euros. It has its headquarter in Bologna and subsidiaries in Milan and Rome.

Since October 2020 HSPI is part of the TXT Group. TXT [3] is a multinational IT group, an end-to-end provider of software solutions, consulting, and services to support the digital transformation of products and processes. With a portfolio of proprietary software and specialized vertical solutions, TXT operates in various markets, with a growing presence in the aerospace, aviation, defense, industrial, government, and fintech sectors. TXT is headquartered in Milan and operates through subsidiaries in Italy, Germany, the UK, France, Switzerland, and the United States of America. The TXT parent company, TXT e-solutions S.p.A., has been listed on the Italian Stock Exchange, at the Star Segment (TXT.MI), since July 2000.

In chapter 2 I briefly expose two of the most widely used approaches to cybersecurity: risk-based and control-based; then, I describe what GRC is in general and how it contributes to risk management.

In chapter 3, I describe the context in which the project took place. After a brief introduction to the customer company profile, I outline the threat profiles of the industry, before describing the preparatory activities that were run before launching the project.

In chapter 4 I describe the tool that was implemented in the project, starting with general information about the platform, before going deeper into the characteristics of the instrument.

In chapter 5 I describe how the project was managed, from the organizational point of view, and the role I played in it.

In chapter 6, I describe the risk model adopted for the project and, in particular, the risk indicators calculated according to the risk model.

The 7th and final chapter describes the project stages, with a particular focus on the activities that I carried out.

2 Background

In this chapter I will first briefly expose two of the most widely used approaches to cybersecurity: risk-based and control-based; then, I will describe what GRC is in general and how it contributes to risk management.

2.1. Common approaches to risk management

There are documents that represent actual standards or de facto standards whose purpose is to provide guidelines for the design of risk management systems, the most important being NIST SP 800-39 (Managing Information Security Risk), ISO 31000 (Risk management - Principles and guidelines), and ISO 27005 (Information security, cybersecurity and privacy protection — Guidance on managing information security risks). For the project described in this thesis, the model adopted is proprietary of the consulting company which lead the project, but it is based upon the guidelines just mentioned.

2.1.1. Risk-Based approach

The risk-based approach to cybersecurity is based on the concept of risk management. This approach is focused on identifying potential risks to an organization's information and assets, and then implementing measures to mitigate those risks. The risk-based approach takes into account the likelihood of an attack occurring, as well as the impact that an attack would have on the organization if it were to occur. This allows organizations to prioritize their cybersecurity efforts based on the most pressing risks that they face.

In the risk-based approach, organizations first identify their assets, such as their systems and data, and then assess the risk to each of these assets. The assessment considers factors such as the sensitivity of the information stored on the asset, as well as the likelihood of an attack. Based on this assessment, organizations can then develop a risk mitigation strategy that is tailored to their specific needs. This strategy may include measures such as implementing firewalls, conducting regular security audits, or providing employee training on cybersecurity best practices.

Risk-based approaches use mathematical models to assess:

- the impact of external threats on the assets held by the organization
- the organization's ability to manage such threats.

Risk-based approaches provide a more "tangible" view of cyber risk, specific to the organization and its context. In recent years, many risk-based frameworks have gained popularity for good reason. They have matured and become more sophisticated, making it possible to measure specific risks and their impact more accurately than ever before. Greater automation is facilitating the monitoring of vulnerabilities, threats, and the effectiveness of controls and countermeasures.

Generally, a risk-based approach is of interest to organizations (especially those of medium size) because the amount of resources allocated to information security is rather limited. The risk-based approach is designed to ensure a correct distribution of resources through:

- the application of the principle of proportionality
- awareness of the value of one's assets and protection requirements
- knowledge of existing controls and countermeasures within the organization
- awareness of threats that could compromise requirements.

2.1.2. Control-Based approach

The control-based approach to cybersecurity is focused on implementing security controls to prevent or detect cyber-attacks. This approach is based on the idea that by implementing a set of well-defined security controls, organizations can prevent or detect attacks before they cause significant damage.

In the control-based approach, organizations first define the security controls that they need to implement, and then develop a plan to implement these controls. The controls may include measures such as access control, encryption, and network segmentation. Once the controls have been implemented, organizations then monitor their systems to detect any potential attacks.

2.1.3. Comparison of the two approaches

The control-based approach to cybersecurity is often seen as a more proactive approach compared to the risk-based approach. This is because it is focused on preventing attacks before they occur, rather than responding to attacks after they have happened. In addition, the control-based approach can benefit from widely available standards and frameworks, such as those made available by NIST or ISO.

On the other hand, the risk-based approach is usually considered more effective in addressing the specific risks of the business and more flexible to adapt to changes in the risk situation, allowing to map more precisely the controls adopted on the identified risks.

It is often believed that a risk-based approach may require more effort and a more skilled project team, particularly in the specific problems of the organization's business.

In conclusion, both the risk-based and control-based approaches to cybersecurity are important for ensuring the protection of an organization's information and assets. Organizations can choose to adopt either approach, or a combination of both, depending on their specific needs and priorities. In this thesis we will deal with both the approaches, because they are both relevant for the project presented here, even if in the development of the project the risk-based approach was privileged, which appeared more appropriate in the specific situation. Consequently, in the following chapters the followed approach will be mainly the risk-based one.

2.2. GRC tools

In the previous chapter we briefly discussed the theoretical principles of risk-based and control-based approaches to cybersecurity. In this chapter we will explore how these principles can be applied in a practical context through the use of GRC tools.

In this chapter we will first introduce GRC tools, their objectives, functionalities, and their pros and cons. Then, we will discuss the application of GRC tools in two areas: IT Cyber risk management (ITRM) and Enterprise Risk Management (ERM).

2.2.1. Introduction to GRC Tools

GRC tools are software applications that integrate governance, risk management, and compliance activities into a single platform. The primary objective of GRC tools is to help organizations achieve compliance with regulations and standards, as well as to manage risks and ensure that governance objectives are met. The functionalities of GRC tools can vary, but they generally include:

- Risk assessment
- Policy management
- Compliance monitoring
- Auditing
- Engagement reporting.

The Risk assessment functionalities support the entire risk assessment process starting from the identification of the main business processes / areas to be considered, passing through the mapping and identification of risks with a clear and immediate representation of the range of threats that can be encountered, up to produce a qualitative or quantitative assessment of the risks and manage remediations plans that allow the reduction of the established risk.

The Policy management functionalities provide a centralized process for creating and managing policies, standards, and internal control procedures that are cross mapped to external regulations and benchmarks.

Compliance monitoring functionalities support organizations in checking how well their business operations meet their regulatory and internal process obligations.

The Audit functionalities involve planning audit engagements, executing engagements and reporting findings to the audit committee and executive board.

Engagement reporting assures key stakeholders that the organization's risk and compliance management strategy is effective. Obviously, the large amount of information that is managed by a GRC involves the need to produce many reports of different nature, from those of a regulatory nature to the directional ones for the company board, to those operational that support the personnel along the different steps of the process; the flexibility of defining and executing reports is essential for the smooth operation of a GRC.

2.2.2. Pros and Cons of GRC Tools

There are several benefits to using GRC tools in risk management and compliance activities. First, GRC tools provide a centralized platform for managing governance, risk management, and compliance activities, which can help organizations save time and resources. Second, GRC tools can help organizations identify and manage risks more effectively, by providing a systematic and standardized approach to risk assessment and management. Third, GRC tools can help organizations achieve compliance with regulations and standards more easily, by automating compliance monitoring and reporting.

However, there are also some potential drawbacks to using GRC tools. First, the implementation of GRC tools can be complex and time-consuming and may require significant investment in terms of both time and resources. Second, GRC tools can be inflexible, as they may not be able to adapt to the unique needs and circumstances of each organization. Third, GRC tools can create a false sense of security, as organizations may rely too heavily on these tools and fail to address risks that are not captured by the tool.

2.2.3. Application of GRC Tools in IT Cyber Risk Management

The use of GRC tools in ITRM can help organizations manage the risks associated with cyber threats and attacks. The risk assessment functionalities of GRC tools can help organizations identify the risks associated with their IT systems and networks, and prioritize them based on their severity. The policy management functionalities of GRC tools can help organizations develop and implement security policies and procedures that are designed to mitigate these risks.

The compliance monitoring functionalities of GRC tools can help organizations ensure that they are complying with relevant regulations and standards, such as the GDPR and the PCI DSS. The reporting functionalities of GRC tools can help organizations demonstrate to stakeholders that they are effectively managing their IT Cyber risks.

In its 2021 Magic Quadrant for ITRM Gartner group predicts that, up from 45% today, by 2023 80% of organizations involved in formal risk management programs will use a ITRM product to manage their IT and cyber risks, with a significant shift towards cloud implementations. For this reason, many GCR providers have transitioned to a SaaS offering.

2.2.4. Application of GRC Tools in Enterprise Risk Management

The use of GRC tools in ERM can help organizations manage the risks associated with their operations and activities. The risk assessment functionalities of GRC tools can help organizations identify the risks associated with their business processes, such as financial reporting, supply chain management, and human resources management. The policy management functionalities of GRC tools can help organizations develop and implement policies and procedures that are designed to mitigate these risks.

The compliance monitoring functionalities of GRC tools can help organizations ensure that they are complying with relevant regulations and standards, such as the SOX and the ISO 9001 quality management standard. The reporting functionalities of GRC tools can help organizations demonstrate to stakeholders that they are effectively managing their enterprise risks.

In this thesis we will focus mainly on application of GRC tool ARCHER, which was used within the project to address Risk Management issues, with a particular focus on IT Risk.

3 Project context

This chapter describes the context in which the project took place. After a brief introduction to the customer company profile, I proceed to outline the threat profiles of the industry. Finally, I describe the preparatory activities that were run before launching the project.

3.1. Company profile

The customer is a group of companies which offer solutions and protection to a few million customers in insurance, banking, real estate, and services sectors, with thousands of employees in Italy and other countries inside and outside of the European community. It shows a high level of solidity, as evidenced by a solvency ratio (Solvency II) near 300%. The company had a profit of hundreds of millions of euros, with a premium income slightly above €5 billion.

The company operates in both the insurance and reinsurance activities in Property and Casualty insurance sector as well as in the Life insurance sector and operates in all LOBs. The company has an agency network, consisting of hundreds of contracted agencies, and tens of distribution agreements, with Credit Institutions, Leasing Companies, and SIMs for the sale of both Property and Casualty and Life policies. The company's premiums are almost entirely generated by direct business, as the premiums from indirect business represent only 0.10% of the total premiums. The percentage of direct business premiums for Property and Casualty insurance was around two thirds of the company's total premiums.

3.2. Threat profiles in insurance and financial sectors

The insurance and financial services sector are constantly targeted by cyber criminals with various motives, not only money driven.

In the following paragraphs we will briefly outline the reason why insurance and financial sector are more exposed than others to IT risk and to the impacts generated by threats, making it particularly important for the whole sector, and for the company we are dealing with here, the adoption of a GRC. [4]

3.2.1. Threats

3.2.1.1. People as a vector of attack

It is well known and documented that most of the attacks begin with social engineering, pretexting, phishing, and insider threats, while many companies spend most of their budget on technological solutions, neglecting this type of extremely dangerous threats.

3.2.1.2. Cyber criminals' continuous evolution

The Verizon Data Breach Report [5] highlights cloud-based attacks double year after year, in line with the increase in teleworkers. Cyber criminals targeting the financial services sector adopt sophisticated strategies, are extremely methodical in their use of tactics, and know their victims well.

3.2.1.3. Supply chain complexity

The supply chain of the insurance and financial sector is extremely articulated, involving a large number of actors external to the company. The risks that come from third party relationship cannot be dealt with within the company, therefore they represent a major source of threat.

3.2.1.4. Specificity of threats for each industry segment

Breach indicators and tactics, techniques, and procedures may vary even deeply in each segment of the industry, so that defenses must be adapted accordingly.

3.2.1.5. New challenges

The rapid evolution of the business, such as in the booming of cryptocurrencies, obliges the companies to quickly adapt their measures of prevention of risk.

3.2.1.6. High stakes

There's particular interest in profiting from an attack directed towards a financial business because of the higher economic return in case of a breach, precisely because the industry rotates around money.

3.2.1.7. High impact

The reputational impact of breaches in financial sector, no matter how big or small the breach is, generally make it to the news, with consequent market reactions that can spread very widely.

3.2.1.8. Specific regulations

Since the sector is regulated by strict norms, the subsequent standardization of processes and procedures facilitates the malicious agent in identifying attack patterns.

3.2.1.9. Legacy technologies

Since finance was one of the first industries to be computerized, with very high investments, it is generally affected by the obsolescence of its information systems, with consequent serious security implications.

3.2.1.10.Complex infrastructure

Over the years, the companies overlapped their systems through merging and acquisitions. This resulted in fragmented and incoherent systems that are difficult to defend, because each of the original components brought their own vulnerabilities.

3.2.1.11.Cloud technologies

Moreover, once the technologies were moved to the cloud, the vulnerabilities, that were previously hidden, became exposed and, therefore, easier to find and exploit.

3.2.1.12.Automation increase

Finally, since to reduce costs and improve services, the insurance companies and financial services firms increasingly rely on automation, introducing new risks due to all the aforementioned issues.

3.2.2. Frequent attack tactics in the insurance industry

According to a research conducted by the computer security company Proofpoint a couple of years previous to this thesis, the most frequent types of attack aimed at insurance, and more in general financial, companies are:

- VBA stomping
- Thread-hijacking
- Weaponized 3rd party authentication
- Multi-layered file-share attack
- "Living-Off-the-land" (fileless/serverless) attacks
- Ransomware-as-a-Service

3.2.2.1. VBA stomping

This technique revolves around spreading (generally through emails attachments) legitimate files, mostly Excel files, that contains malicious VBA macros that present to security analysis engines an executable VBA code different from the one they actually execute. Many code signature and heuristic detection tools are, therefore, tricked and bypassed.

The way in which VBA stomping is carried out consists of removing the VBA source code of a Microsoft Office document, leaving in the document only the compiled version (p-code) of the macro.

The VBA Stomp site [6] provides a conspicuous amount of information on this kind of attack and several ways to protect your company from it.

3.2.2.2. Thread-hijacking

This attack technique injects the content of illegitimate emails (such as malicious URLs) in an existing discussion thread, that is generally trusted by the users involved in it, so that they tend to click the links and fall for the attack.

Another common approach is to inset the malicious URLs inside the previous messages email section, since many security analysis tools, based on the heuristic method, do not check previous messages

Generally, the purpose of the attack is to diffuse other malwares; one of the most notorious and effective malware in achieving success in this kind of attack is the Emotet trojan, very well described, among others, by Kaspersky on their site [7].

3.2.2.3. Weaponized 3rd party authentication

This attack technique allows the attacker to take control of the victim account by altering the DNS to trick users into disclosing the authorization tokens in SAML format to the cloud application of a user (e.g. Microsoft 365). The attack generally begins with malicious emails that redirect to a fake site that seems to be the one that the attacker wants to violate, but is indeed under control of the attacker, where the user inserts its credentials that are intercepted by the attacker. The next step often consists of violating the email account, granting the attacker to use it maliciously even long after the interception of the credentials. Taking control of the email account also grant the attacker the possibility to change the passwords of other application tied to the email address, taking control of those too.

On the MDSec site there is an example of how to build such a tool to reproduce this attack. Trend Micro [8], among others, explains how the attack was effectively perpetuated by Pawn Storm.

3.2.2.4. Multi-layered file-share attack

This technique exploits a document that can be generally found as attachment in an email and that points to other documents kept in different file sharing and that refers to a payload infected by malware.

This process implies that the payload must be activated and this can require many interaction by the user, but it cannot be detected by the defense system that carry out simple documents and emails analysis.

3.2.2.5. "Living-Off-the-land" attack

This attack technique, that does not exploit files or servers, uses the functionalities of the target system, such as Microsoft Office 365, to run its payload, which is not in form of a binary file and can, therefore, bypass the defense measures based on signatures and heuristic analysis.

In Microsoft environment, a famous attack of this kind is the CVE-2017-8570, that is precisely described, among others, on the Trend Micro site [9].

3.2.2.6. Ransomware as a Service

Ransomware is evolving toward becoming RaaS, already largely available on the dark web: crackers focus on developing software and leave attackers the task of identifying the potential victims and deploy the malicious software. RaaS enables unskilled people the possibility to launch ransomware attacks by subscribing to a service.

A simple but exhaustive description of RaaS is provided, among others, by Telsy on their site [10].

3.3. Preparatory activities for the Project

Before the implementation of the project the client company already formally managed governance, risk and compliance, both for business reasons and regulatory obligations, but did not have a GRC system. Therefore, risk indicators were managed using, partially, business information coming from a process management system (ARIS by Software AG [11]) and afterwards, heavily manipulated manually on electronic spreadsheets. This resulted in heavy and costly manual activities with consequent high risks of errors, difficulties in identifying and resolving those same errors, poor standardization of activities, risks of delays, organizational tensions between company sectors, etc.

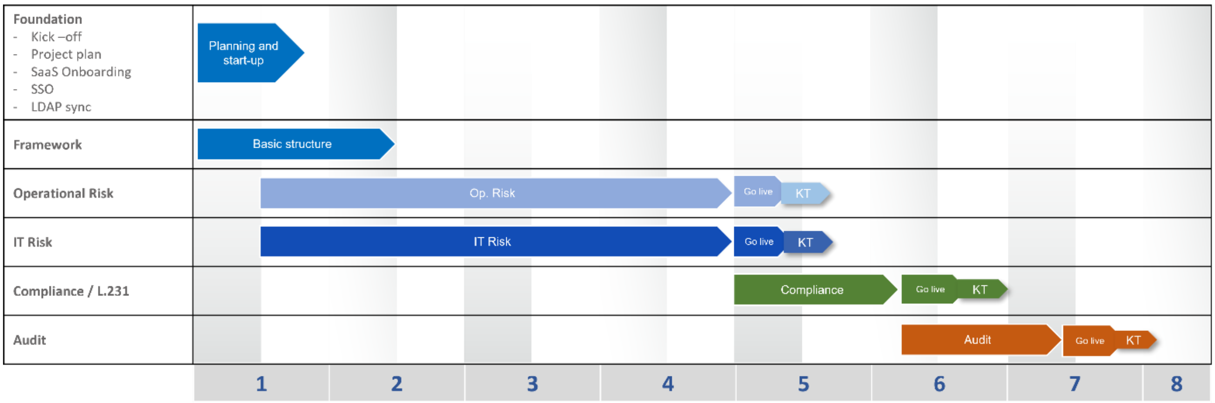


Figure 1: High level preliminary project plan

To solve this situation, the company launched a program of adoption of a GRC tool, that involved a thorough high-level requirements analysis, which was used to compare different leading industry products and ended with the choice of the Archer product.

A preliminary project plan at a very high level was defined as pictured in Figure 1.

Given the complexity of the issues and the strong configurability of the product, the company decided to launch an implementation project involving an IT Governance specialized consulting company (HSPI S.p.A.), where I worked as an intern, which commissioned Archer consulting professionals for specific product configuration activities.

4 Archer GRC

In this chapter I describe the tool that was implemented in the project, starting with general information about the platform, then I explain what integrated risk management is in general before going deeper into the characteristics of the instrument.

4.1. About Archer

Archer [12] is a GRC software developed by the homonymous company, previously owned by RSA Security, the well-known cybersecurity and digital risk management company, specialized in encryption and authentication. Archer was founded in 2001 and counts more than a thousand customers, ranging from small companies of less than a thousand employees to global multi-nationals in the most diverse sectors, spread around the globe. More than 80% of the customers integrate more than one risk domain on the platform.

Archer is a (nearly) zero-code platform that provides all the tools needed for risk management with a simple configuration with a RAD approach; details such as look and feel, module layout, field configuration are often easier to configure on the platform than to document.

4.2. Integrated Risk Management

Archer offers an IRM approach to risk management allowing a company to encapsulate the full spectrum of risk management capabilities:

- Archer enables to address all risk domains in a single configurable platform
- Archer eases business collaboration by offering access to the platform through many different devices, including mobiles, ensuring the availability of the information
- Archer assures the integration with business systems and operational data by providing multiple integration methods
- Archer allows the creation of effective reports to highlight risks and determine management strategies.

4.3. Archer entities

Archer organizes the risk management in a pyramid of entities. [13]

4.3.1. Fields

At bottom level we have fields. Fields hold data provided by users or the system itself. New fields can be created in any application and can be reconfigured by a user with administrative access. Each field type carries a unique set of configuration options, these types can be summarized in two categories:

- System fields: these include history, tracking and status information
- Operational fields: these are the custom fields and include both basic data types such as text, numeric, value list, date and more advanced data types such as cross-references, record-permissions, sub-forms and many others.

4.3.2. Sections

Fields are organized into sections. Sections can be expanded or shrunk from the visualization and hidden or shown according to rules based on domains and roles.

4.3.3. Application

Each collection of related items is housed in an Application. Preconfigured applications are sold as out-of-the-box or core applications. On-Demand Applications are empty applications that can be custom built.

Examples of applications are:

- Finding
- Risk Register
- Remediation Plans.

4.3.4. Solution

Groups of applications that solve a business need are provided as Use Cases by Archer but functionally grouped together in the system as Solutions.

Finding and Remediation Plans applications for example could be found in the Audit Execution solution, while the Risk Register could appear in the Risk Management solution.

4.4. Off the shelf and customized solutions

The product comes with several built-in use cases that can be bought alongside the main platform in order to provide an off the shelf solution. These include applications for the various risk domains, reports, notification systems, etc. developed incorporating the industry-leading best practices in integrated risk management.

However, the platform is completely customizable, starting from scratch or from the use cases mentioned above. Every aspect of the platform is customizable, from the formulas to the user actions, from the reports to the custom objects. These features will be analyzed later in this chapter.

4.5. Risk Informed Decision Making

As summarized in Figure 2 [14], in order to achieve risk informed decision making through an IRM system, Archer aims to enable:

- Productivity and Efficiency: the increment in productivity and efficiency is estimated by Archer to be in the order of 130.000$ per 1000 employees

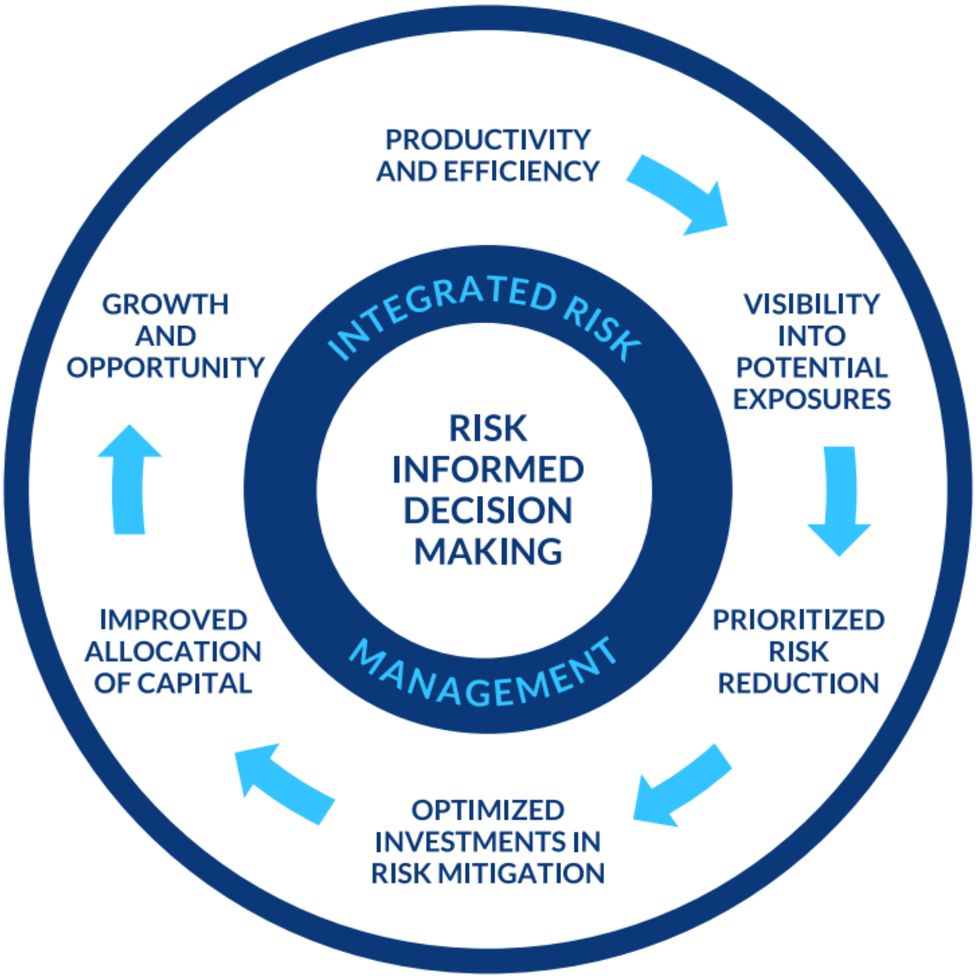

PRODUCTIVITY AND EFFICIENCY
VISIBILITY INTO POTENTIAL EXPOSURES
PRIORITIZED RISK REDUCTION
OPTIMIZED INVESTMENTS IN RISK MITIGATION
IMPROVED ALLOCATION OF CAPITAL
GROWTH AND OPPORTUNITY
INTEGRATED RISK MANAGEMENT
RISK INFORMED DECISION MAKING

Figure 2: Archer approach to IRM

- Visibility into Potential Exposures: Archer handles multiple dimensions of risk on a single platform, creating a coherent management strategy that provides economies of scale and better utilization of data and processes across risk management functions
- Prioritized Risk Reduction: Thanks to the adoption of a centralized platform like Archer, the risk management lifecycle is optimized in all its aspects
- Optimized Mitigation Investments: By quantifying the risk and improving the loss exposure estimations, Archer permits better investments prioritizing in risk mitigation
- Improved Allocation of Capital: Reducing the risks also improves the rating of the organization allowing to an easier access to investments
- Growth and Opportunity: The company can use the integrated risk management program implemented with Archer as proof of its clearance of strategies in the fields of Operational Risk, ESG, Compliance, IT risk, etc.

4.6. Archer main features

4.6.1. Centralized repository for data

Archer allows organizations to collect, store, and manage data on various types of risks, such as cybersecurity, financial, operational, and reputational risks, among others, in a single repository. By centralizing data in Archer, organizations can have a holistic view of their risks and easily access and analyze the data for risk management purposes.

Overall, Archer serves as a central hub for risk-related data, providing organizations with a comprehensive and secure platform for risk management.

4.6.2. Formal description of business processes

Archer can integrate all the levels of the value chain that can potentially present some risks. The processes can be represented in detail from the macro process to the activity to whom the risks are mapped.

A typical process structure that could be implemented in Archer is represented in Figure 3:

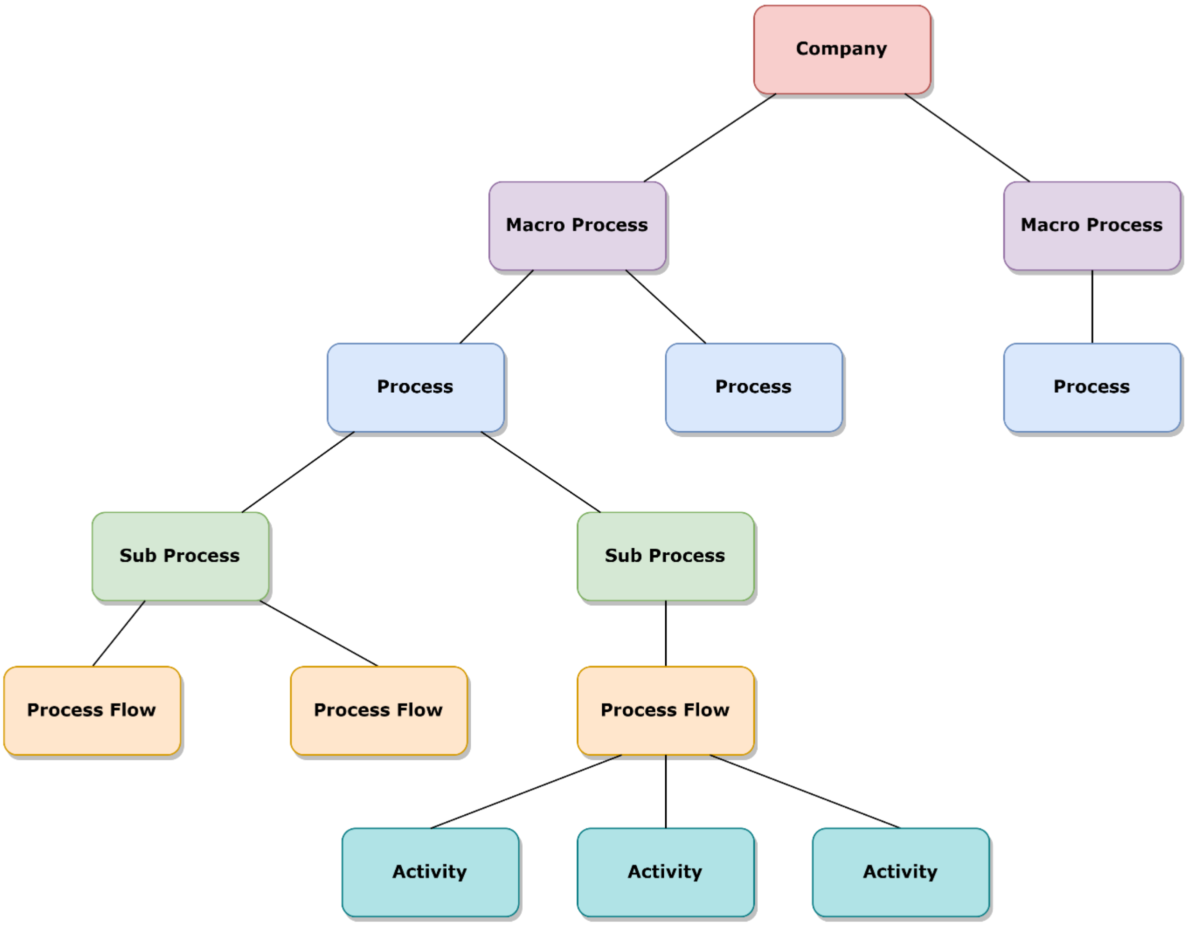


Figure 3: Process structure

4.6.3. Use by multiple areas across the business

The different business units affected by a process can share the risk management information system, according to the specific roles in the process.

4.6.4. Access to data tightly controlled based on user roles

Access control is based upon three level of permission:

- Role: determines what a user can access or not access
- Group: allows to assign permissions to multiple users at the same time
- Record permission: grants specific authorization on the data, and specifically reading, updating and deleting.

This approach allows a very detailed access control to the level of the single application.

There are two ways of accessing the platform:

- through Archer internal identity manager

- through single sign-on via the enterprise LDAP.

4.6.5. Powerful instruments for reporting and dashboard creation

Thanks to a user-friendly interface, that does not require any programming, every user can create and save personal reports and graphics based on their access permissions. Reports administrator for specific applications can build global reports accessible to any user allowed to access the report data.

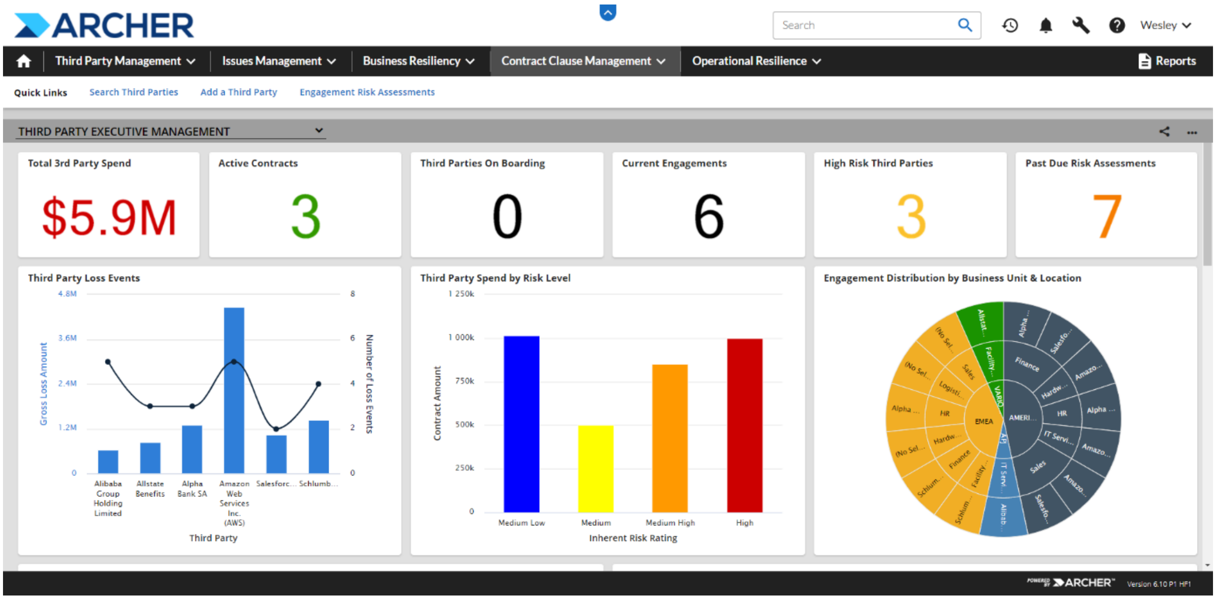
Archer gives powerful tools to search for the desired data by filtering, sorting, rolling up, drilling down and apply mathematical functions to the reports.

Reports can be statistical or not, but only statistical reports can be plotted as charts and include mathematical functions.

System administrators can organize the reports inside dashboards (see Figure 4) that make the most useful information immediately evident to the users.

4.6.6. Deploy On-premises or as a hosted (SaaS) environment

An instance of Archer can be installed On-premises or accessed via SaaS. The cloud-based version guarantees many advantages such as constant updates of the platform by the Archer team and agile access from any device, included in the monthly subscription, whereas traditional On-premise users need to spend up to 20% of the purchase cost annually in maintenance and support fees.



Total 3rd Party Spend	Active Contracts	Third Parties On Boarding	Current Engagements	High Risk Third Parties	Past Due Risk Assessments
$5.9M	3	0	6	3	7

Figure 4: Dashboard example

Both On-premises and SaaS version of Archer offer a SQL Server back end that backup the information daily, allowing to restore the data in case of need. Only the On-premises instances allows the administrators to access the SQL Server database.

4.6.7. Integration with other data-collection systems

The platform enables data integration from various sources, such as internal systems, third-party tools, and external data providers, to guarantee a comprehensive view of risks.

This feature is particularly useful to automate dialogue between the company's system and those of the control agencies that collect the data and will prove increasingly important as the automation of control agencies develops.

4.6.8. Automation

Archer provides a series of automation mechanisms to improve the company's productivity such as:

- Periodic import of data from other platforms through data feeds
- Completion of records through scheduled bulk actions
- Generation of data through bulk create actions
- Event based and scheduled notifications.

4.6.9. Workflows

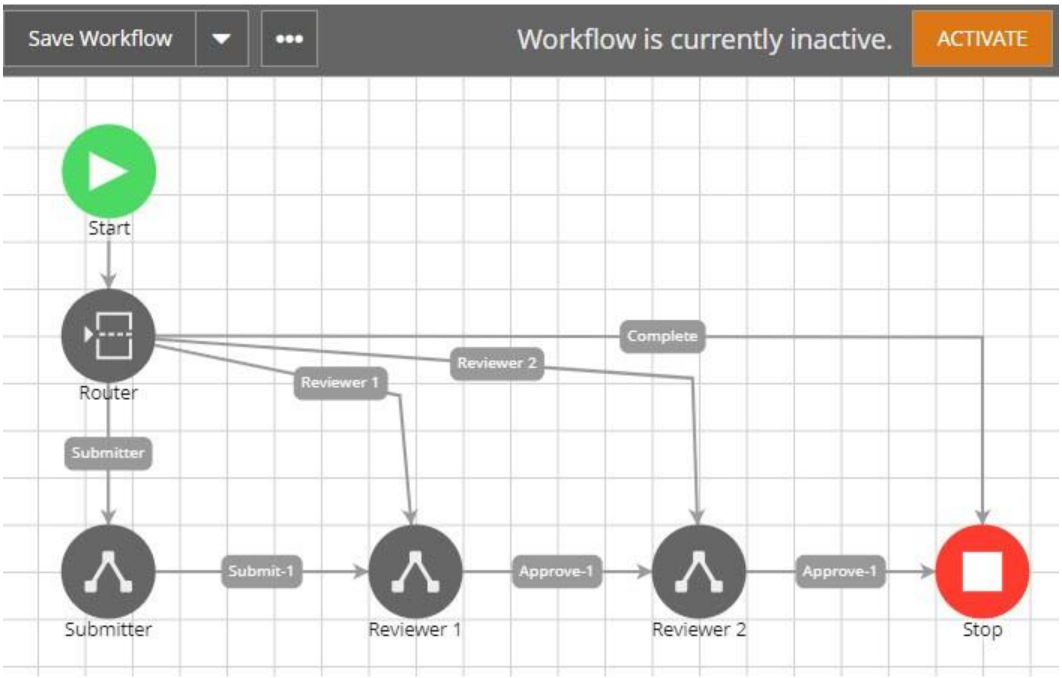


Figure 5: Workflow example

The Archer *Advanced Workflow* feature ensures that the appropriate stakeholders follow the correct business process.

Workflows are designed through a very intuitive graphical interface (see Figure 5) that does not require any coding effort.

The Workflow rules, defined through field evaluation, strongly interact with the actual data contained in the database.

5 Project organization

This chapter describes how the project was managed, from the organizational point of view, and the role I played in it.

5.1. Organization scheme

The Archer implementation project is managed through a formal organization and process that follow the international project managing best practices such as those recommended by PMI. The responsibilities are shared among the customer company and HSPI consulting.

The organizational structure is represented in Figure 6.

5.1.1. Steering Committee

The steering committee includes some of the top-level managers of the customer company and exercises strategic control over the project through periodic meetings in which the people responsible for the project's implementation provide the committee with updates on the progress of the work, any critical issues that have emerged, and any actions that need to be taken.

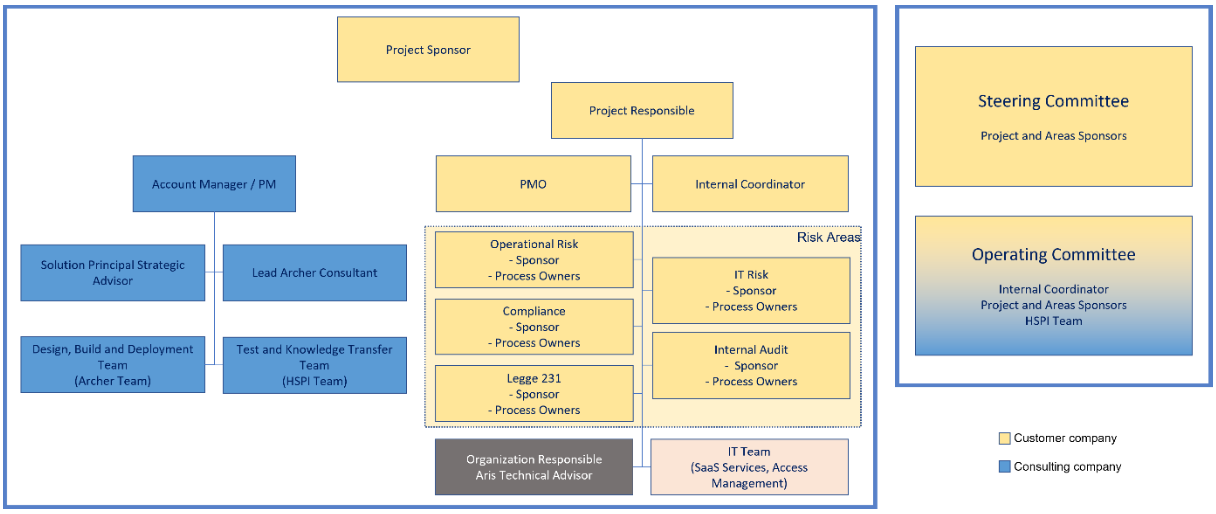

Project Sponsor
Project Responsible
Account Manager / PM
PMO
Internal Coordinator
Solution Principal Strategic Advisor
Lead Archer Consultant
Risk Areas
Operational Risk - Sponsor - Process Owners
IT Risk - Sponsor - Process Owners
Compliance - Sponsor - Process Owners
Internal Audit - Sponsor - Process Owners
Legge 231 - Sponsor - Process Owners
Design, Build and Deployment Team (Archer Team)
Test and Knowledge Transfer Team (HSPI Team)
Organization Responsible Aris Technical Advisor
IT Team (SaaS Services, Access Management)
Steering Committee
Project and Areas Sponsors
Operating Committee
Internal Coordinator
Project and Areas Sponsors
HSPI Team
Customer company
Consulting company

Figure 6: Organizational structure of the project

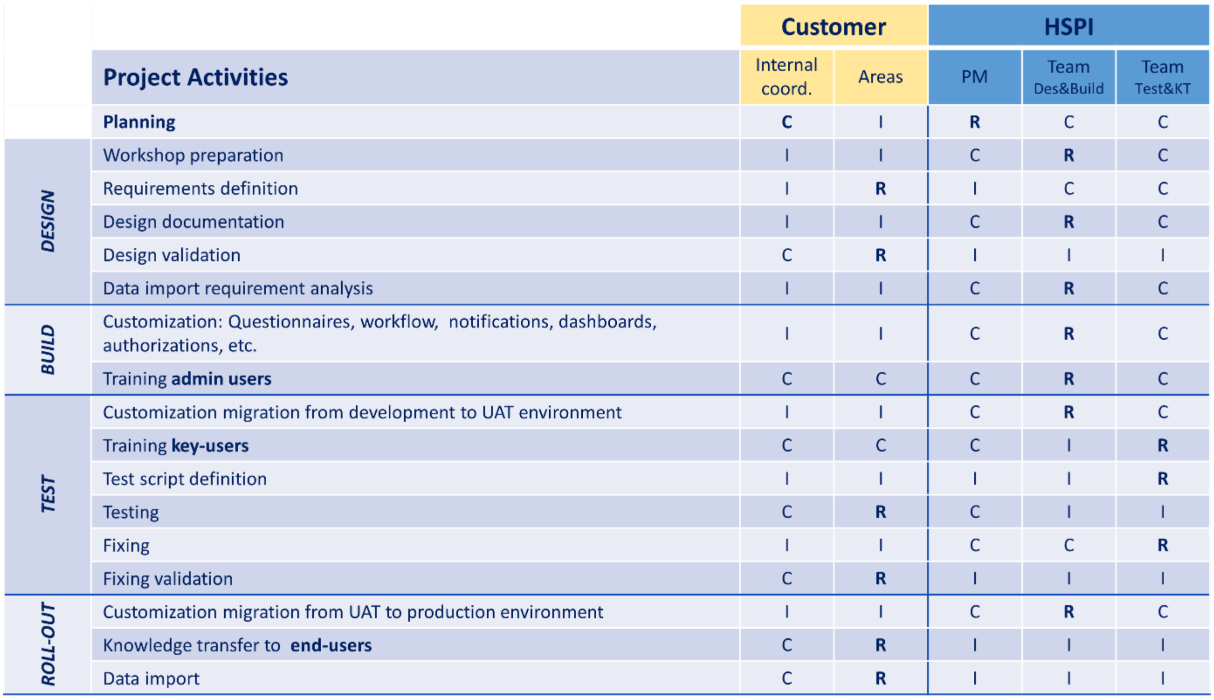
5.1.2. Operating Committee

The operating committee is formed by both members of the customer company and the consulting company. It is responsible for reviewing, overseeing, and guiding the overall operations of the project. The operating committee convenes on a regular basis to address company issues and provide feedback or recommendations to senior and executive management. The operating committee does not directly manage day-to-day operations, but rather focuses on strategic-level operational functions.

5.1.3. Operations

The operational activities are divided between the customer company personnel and the consulting team according to the respective competences, as shown in the RACI matrix, which highlights the Responsible, Consulted and Informed roles within the project. The Accountable figure is not taken into account in Figure 7.

In particular, under the customer responsibilities lie the requirements definition, design validation, testing, end-users training and data import from their systems. The involved personnel are mainly made up of key users responsible of the various domains with global access to the different legal entities. They all act under the surveillance of an internal coordinator and a PMO who both respond to the project manager.



		Customer		HSPI		
	Project Activities	Internal coord.	Areas	PM	Team Des&Build	Team Test&KT
	Planning	**C**	I	**R**	C	C
DESIGN	Workshop preparation	I	I	C	**R**	C
	Requirements definition	I	**R**	I	C	C
	Design documentation	I	I	C	**R**	C
	Design validation	C	**R**	I	I	I
	Data import requirement analysis	I	I	C	**R**	C
BUILD	Customization: Questionnaires, workflow, notifications, dashboards, authorizations, etc.	I	I	C	**R**	C
	Training **admin users**	C	C	C	**R**	C
TEST	Customization migration from development to UAT environment	I	I	C	**R**	C
	Training **key-users**	C	C	C	I	**R**
	Test script definition	I	I	I	I	**R**
	Testing	C	**R**	C	I	I
	Fixing	I	I	C	C	**R**
	Fixing validation	C	**R**	I	I	I
ROLL-OUT	Customization migration from UAT to production environment	I	I	C	**R**	C
	Knowledge transfer to **end-users**	C	**R**	I	I	I
	Data import	C	**R**	I	I	I

Figure 7: RACI matrix

Under the consulting responsibility, instead, lie the planning, design, implementation, training of customer administrators and key users and bug fixing. The consulting team is expert in both risk and project managing and Archer configuration.

5.2. Project planning

As shown in (Figure 8), the project time-lapse from the kick-off to the deployment in production environment (roll-out) was planned to take nine months. After the roll-out, it is agreed for the consulting team to provide Application Maintenance Support for the platform. For the sake of clarity, the first three months of application maintenance were included in the Gantt regarding the implementation project.

The Gantt represents the project at a high-level; a small detail of the activities of each step is contained in the RACI of Figure 7; obviously in daily operations and in the SoW plans of much greater detail have been adopted.

The project was divided into different executive streams, as represented in Figure 8, one for each relevant domain; the streams realization was scheduled according to the urgency of the roll-out of the system for each domain.

After an indispensable preliminary technical setup of the system, we proceeded with the creation of the reference framework to which the different areas must adapt. The implementation of the framework is a complex activity, which requires a strong commitment especially on the part of consultants, and which conditions the development of other areas. By adapting Agile implementation logics to the use of a

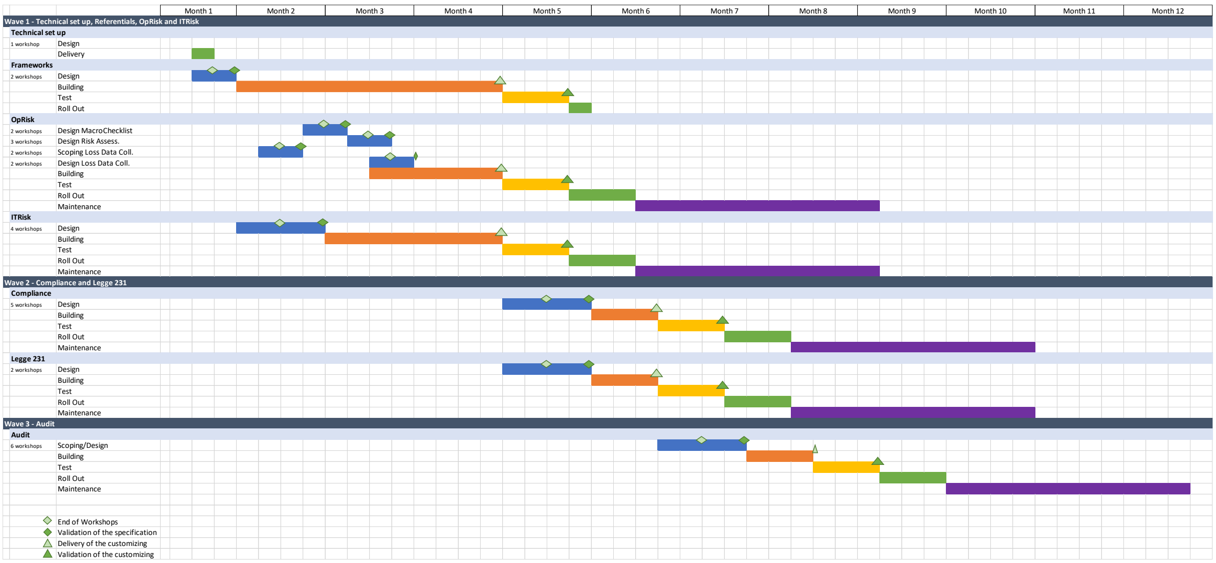


Figure 8: High level project plan

system that does not require code development, the project team quickly and frequently released small components of the framework, even if not complete, which allowed to anticipate as much as possible the start of activities on the most critical streams and the parallelization of activities on different streams.

Within the streams, on the other hand, a more traditional approach (cascade) was maintained, having to ensure that every implementation decision taken by the work team was completely share, understood and approved by the users of the system (in the Gantt the main milestones that allowed the transition from one step to the next are highlighted). This resulted in slightly longer roll-out times, but ensured that the need for Application Maintenance Support was minimized immediately after the roll-out. It also facilitated the roll-out of the project results from the first pilot legal entity in Italy to the other legal entities of the group in other countries and in other languages (for reasons of concision these activities are not highlighted in the Gantt).

The Application Maintenance Support of the project essentially concerns corrective problems and small evolutions, which do not require a design approach.

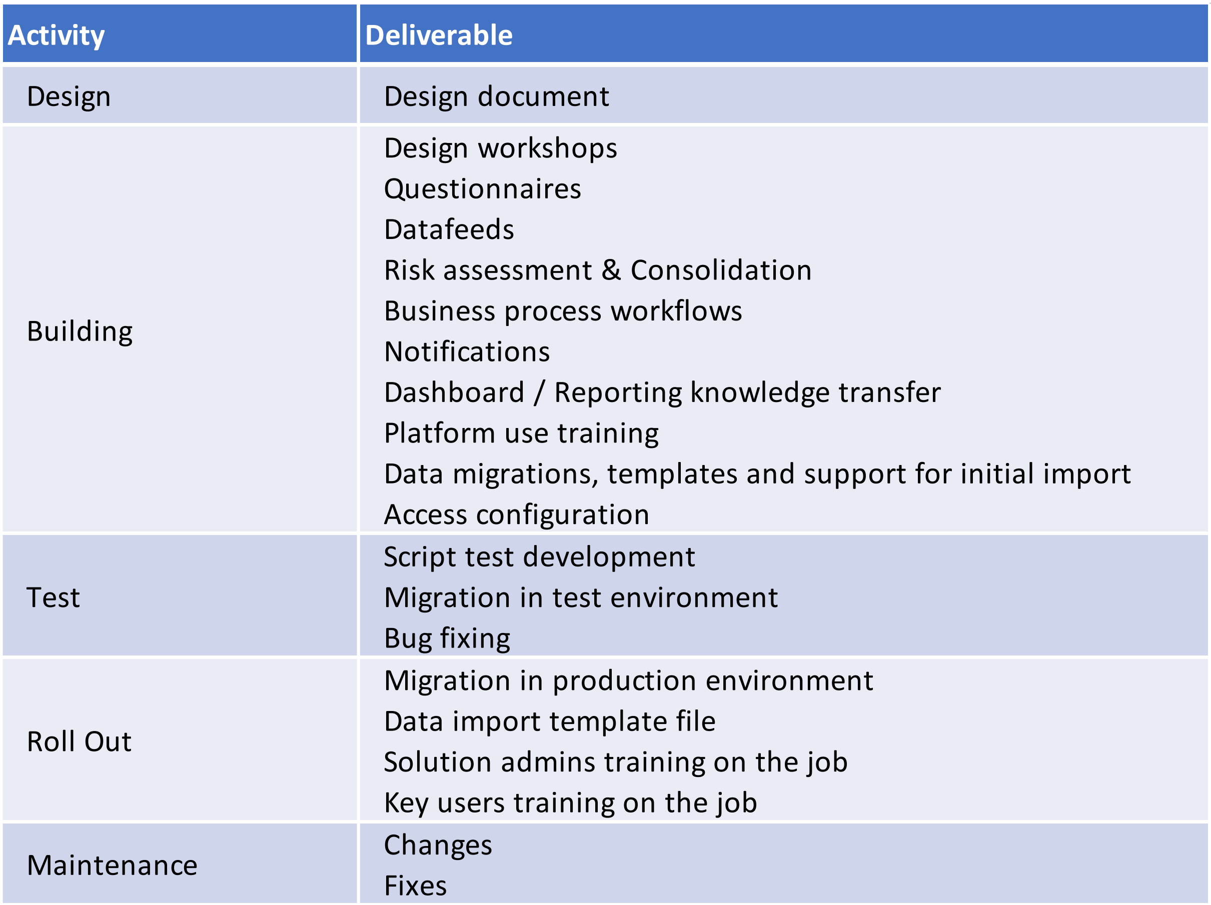
The Gantt highlights that the prevailing activity results in the building. This depends on the massive customization of the system, required to meet the customer needs.

5.3. Deliverables

Each activity of the project produces some deliverables that the consulting team shares with the customer during the project meetings.

The table in Figure 9 gives an idea of the types of deliverables that are produced for the main activities.

Each of those deliverables is then specifically adapted to each domain of the project (i.e., IT risk, compliance, etc.).



Activity	Deliverable
Design	Design document
Building	Design workshops Questionnaires Datafeeds Risk assessment & Consolidation Business process workflows Notifications Dashboard / Reporting knowledge transfer Platform use training Data migrations, templates and support for initial import Access configuration
Test	Script test development Migration in test environment Bug fixing
Roll Out	Migration in production environment Data import template file Solution admins training on the job Key users training on the job
Maintenance	Changes Fixes

Figure 9: Project deliverables

5.4. My role in the project

My internship began with the project already being in progress. In particular, before I joined the team, the technical setup was completed and the framework was partially implemented. Some solution areas were already in the test phase, while others were still in design or building phase.

In the operational risk area, I took part in the testing activities and everything that followed, with particular focus on the users training in the roll out stage.

For what concerns IT risk, I was involved in refining the design and the calculation model, before facing the tuning of the configuration and the test and roll out. I took part in populating the environments and fixing the bugs, as well as in designing and building application changes.

Regarding, the compliance (including both standard compliance and Legge 231), as for operational risk, I started during the test phase and I had a major role in the data population and reporting for the roll out phase.

The internal audit part of the project started after my involvement in the project, but I mostly participated in the bug fixing, after the testing phase, and the translation.

For all the solution areas, as of when this thesis is written, I am involved in the maintenance.

6 Risk model

In this chapter, I describe the risk model adopted for the project, that follows the custom methodology proposed by HSPI, which has its roots in the risk based approach. In particular, I will briefly explain the risk indicators calculated according to the risk model.

In general, risk (R) is calculated as follows:

$$R = P \times I$$

where:

P = probability

I = impact

We considered three risk views: inherent (or gross), actual (or net) and residual.

6.1. Inherent risk

Inherent risk (Rintr) is the type of risk calculated in the absence of countermeasures.

For the calculation of the inherent risk two components are considered:

- Inherent probability (Pintr)
- Inherent impact (Iintr).

1. Inherent probability (Pintr)

$$P_{intr} = P_{car} + O_{fdc}$$

where:

Pcar = probability characteristic of each threat

Ofdc = offset calculated on each context factor.

Let's analyze the two components of this formula (on Archer that is made in “Application IT Assessment”).

- Probability characteristic of each threat (Pcar)

A characteristic probability value is attributed to each threat, representing how likely a threat may occur.

This value is on a five-level scale (very low, low, medium, high, very high) and each level corresponds to a number from one to five and N/A if the threat is not applicable.

- Context factors (Ofdc)

They describe the different services within the same organization, and not all context factors affect all threats.

They act as an offset of the characteristic probability and each factor has its own possible responses that are closely related to the context factor.

  - decreases the probability of occurrence of a threat
  - increases the probability of a threat occurring.

One could possibly weigh the context factors, i.e. say which one is worth more, but right now in the system they are all worth 1.

2. Inherent impact (Iintr):

It corresponds directly to the values attributed to the 11 consequences, and it is represented on a five-level scale (from very low to very high) or N/A in the case of non-applicable consequences.

In order to carry out the calculation of the inherent risk (Rintr), we need to define a mapping between threats and consequences.

In fact, threats have only the probabilistic components, while the consequences have only the impact components.

For the calculation of the inherent risk, we need both components and therefore we will have to map the threats with the consequences (just to understand which couples exist and which do not). We must calculate the risk only for those couples that exist.

We can consider the inherent risk according to three points of view:

1. Aggregate risk

The aggregate risk (Raggr) is the total risk over the entire service and is calculated as follows:

$$(\text{Raggr}) = \text{Paggr} \times \text{Iaggr}$$

where:

Paggr = aggregate probability; it is the average of all probabilities of each couple

Iaggr = aggregate impact; it is the maximum possible impact (highest value).

2. Risk by consequence

The risk per consequence (Rcons) is the one with the focus on the consequences and is calculated as follows:

$$(Rcons) = Pcons \times Icons$$

where:

Pcons = probability per consequence; it is the average probability of all threats applicable to each consequence

Icons = impact per consequence; it is the inherent impact (Iintr) calculated for each consequence.

3. Risk by threat

The risk per threat (Rthr) is the one with the focus on threats and is calculated as follows:

$$(Rcons) = Pcons \times Icons$$

where:

Pthr = probability per threat; it is the inherent probability (Pintr) calculated for each threat

Ithr = impact per threat; is the maximum possible impact applicable to the threat (highest value)

The mitigation factor (FdM) is the percentage of decrease of the inherent probability and inherent impact components to transform them into actual probability and actual impact.

We do not calculate an amorphous mitigation factor, but we identify what are the components of the service (in Archer: IT Application), i.e., all the individual bricks that make up a service (in Archer: the Components).

The service is composed in a nutshell of an application part and an infrastructural part (in turn formed by networks, systems, physical part).

During the project we identify which are the components to be linked to our application, in the form of instantiated templates, then we identify the templates referring to a specific asset or business process.

Once identified the correct templates, we link them to the components and we carry out the evaluation of countermeasures. E.g. let's suppose to evaluate the XXX application, composed of many components (e.g.: XXX1, XXX2, etc.); we will link the components to the XXX application and evaluate one by one the controls within the components.

Controls have four attributes:

1. Nature

- preventive (in Archer: "probability")

Knocks down the probability for threats to happen (e.g. access controls)

- reactive (in Archer: "impact")

Once a threat has occurred, it mitigates its impact (e.g. backups or incident management controls)

- both.

2. With which threats is a countermeasure mapped

Not all countermeasures equally mitigate all threats. Some countermeasures mitigate some threats (e.g. access controls mitigate ransomware or phishing, but not theft of paper documents, that are instead mitigated by physical countermeasures).

3. With what consequences a countermeasure is mapped

Not all consequences equally mitigate all threats. Access control measures mitigate consequences of unauthorized access to data, but do not mitigate consequences of data loss, that are instead mitigated by backup.

4. Weight

The more control weights, the more it will affect the mitigation factor.

The crossing of these four attributes determines the mitigation factor.

For all couples (threats - consequences) we calculate the mitigation factor of probability and impact.

Archer's calculation system generates tuples (or 5-dimensional matrix), whose dimensions are:

- Threats
- Consequences
- Nature
- Components
- Controls.

So, we will have as many rows as these five dimensions are.

In addition, each tuple contains for each cell the answer given by the Custodian (0 if the control is very bad, 1 if the control is excellent).

The tuple also shows the cluster control values (CCV), i.e. the weighted average of the evaluations of the controls that comply with the tuple criterion. Executing this step we eliminate the couples consequences - threads that are not eligible on the basis of a matrix defined during system customization.

For each tuple that is eligible, we calculate the mitigation factor.

Depending on the nature, the formula changes because:

- If it is preventive, the mitigation factor is calculated as follows:

$$FdM = (0.9 \times CCV) / 5$$

- If it is reactive, the mitigation factor is calculated as follows:

$$FdM = (0.5 \times CCV) / 5$$

Factors 0.9 and 0.5 were agreed between customers and consultants during system design: the probability can be mitigated by a maximum of 90% and the impact can be mitigated by a maximum of 50%.

For each of these tuples therefore we know the inherent risk, given by the threat and the consequence.

6.2. Actual risk

The actual risk (Reff) is the type of risk that shows a snapshot of the current situation, therefore in the presence of countermeasures, leading to the calculation of the actual risk.

The calculation of the actual risk (Reff) depends on the nature:

- if it is preventive, the FdM applies it to probability, therefore:

$$R_{eff} = P \times (1 – FdM)$$

- if it is reactive, the FdM is applied to the impact, then:

$$R_{eff} = I \times (1 – FdM).$$

In Archer are loaded

- inherent and actual probabilities and impact for each component, threat and consequence
- actual probability and impact for each application.

6.3. Residual risk

From the calculation point of view Residual risk (Res) works the same way as Actual risk, but while Reff represents my current situation, Res represents instead the future situation I want to obtain, defining which level of risk I can manage.

We must not aim to eliminate the risk altogether, as this is practically impossible, but to manage it, that is, to get to that point where managing risk is more cost-effective than trying to eliminate it.

There is a clear relationship between costs and benefits.

- If it is preventive

$$Rres = P \times (1 – FdM)$$

- If it is responsive

Rres = I x (1-FdM).

7 Implementation of Archer

This chapter describes the actual project phases, through the analysis of the methodologies adopted and the obtained results, with a particular focus on the activities that I carried out. The project aims to manage the client's overall business risk, by handling both cyber risk and enterprise risk from a single application. However, my work within the project has been mainly focused on, though not exclusively, the IT risk area. Therefore, I will principally describe the implementation process of this area, which is also of greater interest for the thesis subject being computer security.

The implementation of the IT risk stream was characterized by the macro activities mentioned at the end of the previous chapter:

- Design
- Building
- Test
- Roll out
- Maintenance.

7.1. Design

The design phase began with the consolidation of high-level requirements, which were drafted in the pre-project phase as guidelines for the project itself, and the definition of detailed requirements. Both company employees, as well as the consultant team process experts, participated in this activity. Archer's expert consultants played a validation role for the requirements to determine their coherence with the features available on Archer.

The activity was carried out through workshops, formal and informal discussions, exchange of information via email, and sharing of project documentation. The involvement of company personnel and interaction between users and consultants was very strong throughout the activity.

The results of this activity were formalized in a Requirements Analysis document, which constituted the starting point for the subsequent Building phase. The

Requirements Analysis was discussed in the project's operational committee, and a summary was presented to the steering committee.

The main result of the design phase is the risk model; as previously mentioned, the risk model adopted is proprietary of HSPI S.p.A., but it is based upon the ISO guidelines and adapted to Archer features.

In the following pages I describe the main elements of the implementation:

- Entities
- Campaign life cycle
- Risk calculation process.

7.1.1. Entities

The central entity around which the system is implemented is the IT application, considered as a whole, taking into account both the application-related aspects as well as the infrastructure, operational, and procedural aspects.

The data model in Figure 10 gives an overview of the objects and the connection in the scope of the IT risk. Some connections are not represented (example: link between the IT campaign and the questionnaires) and will be described later on.

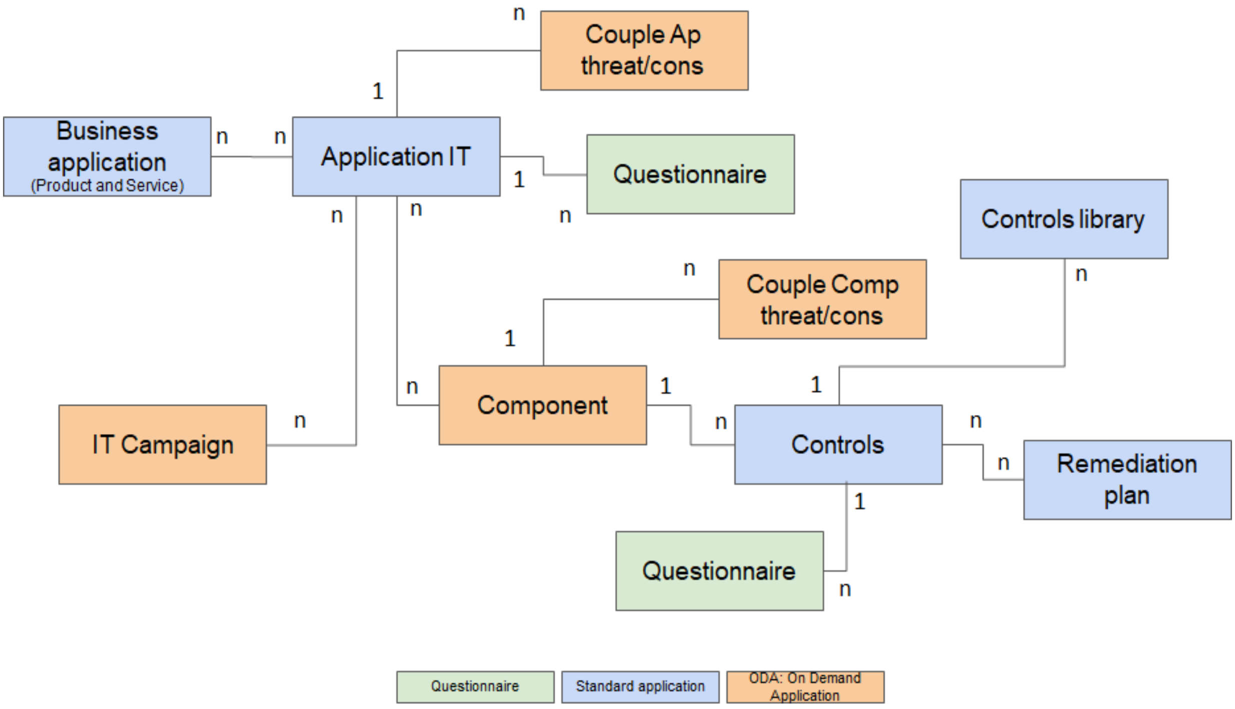


Figure 10: Archer ITRM data model

7.1.1.1. IT application

IT applications represent the main assets of the company in the risk-based approach described in the first chapter.

An IT application is a software system used by employees of the company to automate business processes and activities. Each IT application can be linked to many business applications, each of whom can be related to different IT applications. For instance, the "Ricerca Anagrafica" IT application is linked to many business applications, that make use of it, such as "App di Firma", that on its behalf uses other IT applications such as "Firma Digitale". The Business applications directly come from Aris.

An IT application is characterized by various fields, some of them are set manually, others are generated by the system based on configuration rules, and the remaining ones are automatically calculated by the risk management processes.

The manually filled field values can be set freely or assume fixed values according to the product configuration. For example, the user responsible of the application can be selected from the list of users belonging to a particular access control group. On the other hand, the description of the application is a free text field.

The reference field to the threat-consequence couples is an example of the second type of field, since the couples are instantiated by a data feed at the time of creation of the application based upon templates uploaded during the system configuration.

The last kind of field is calculated at runtime while the data evolves. The most obvious example of this type of field is the risk value.

7.1.1.2. Component

Components are the bricks that build the IT applications. There are specific application components, homonymous to the application itself, and other components that belong to different applications.

Components are based on templates created or uploaded during the system configuration. From these templates the components inherit the controls.

An important attribute field for components is their weight, since this characteristic affect the risk calculations.

7.1.1.3. Control

As well as components, controls have a weight that affects, in their case, the mitigation of the inherent risk and a reference template, called "Control library", from which the controls inherit:

- The affected element: probability, impact or both
- The mapped threats and consequences.

The most significant fields of controls are the control maturity, depending on the most recent control questionnaire, and the target maturity, related to the remediation plans.

Controls are mapped onto the components' templates, and therefore linked to the instances of components.

7.1.1.4. Threat-Consequence Couple

There are two types of threat-consequence couples: those mapped to the IT applications and those mapped to the components.

The instances of this entity are clones of the master level couples, from which they inherit the threat and consequence values. This entity too has a field that defines its weight in the risk calculation.

As calculated fields, couples present threat and consequence mitigation factors for effective and residual risk.

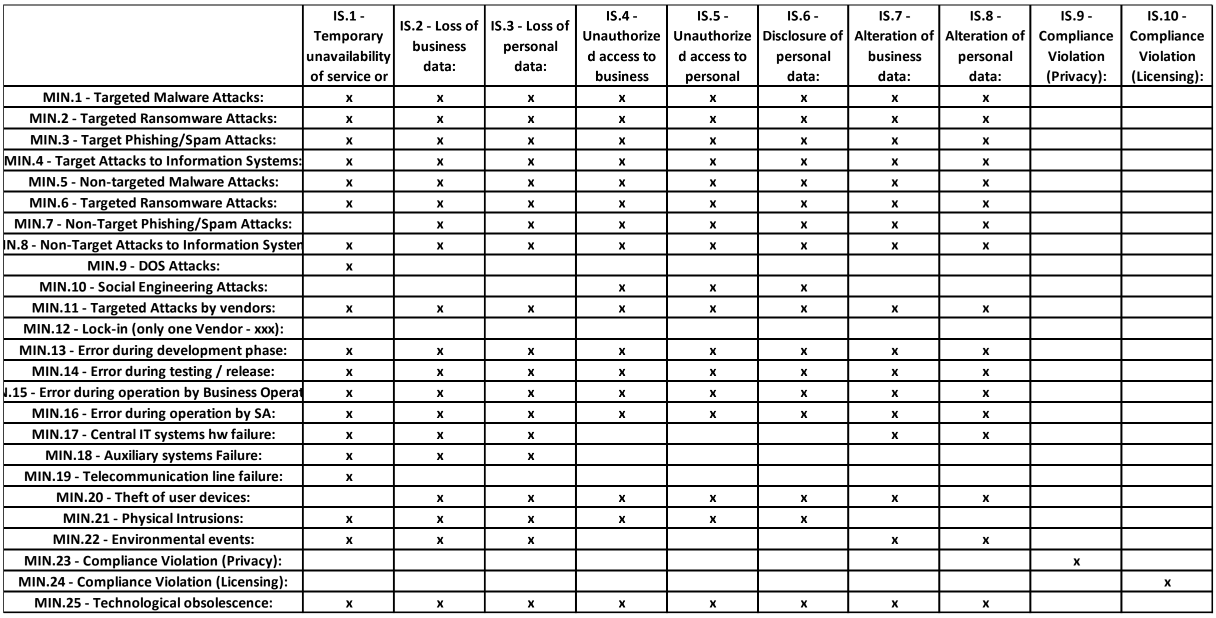
In Figure 11, an example of coupling between threat and consequence.

7.1.1.5. IT Risk campaign

IT risk campaigns are launched periodically (every quarter) by the IT risk administrator, who selects a user responsible for a campaign.

Campaigns include IT applications in their scope and present a start and end date.

The launch of an IT risk campaign causes the generation of questionnaires; one for the IT Application and one for each control mapped onto the components in scope.



	IS.1 - Temporary unavailability of service or	IS.2 - Loss of business data:	IS.3 - Loss of personal data:	IS.4 - Unauthorized access to business	IS.5 - Unauthorized access to personal	IS.6 - Disclosure of personal data:	IS.7 - Alteration of business data:	IS.8 - Alteration of personal data:	IS.9 - Compliance Violation (Privacy):	IS.10 - Compliance Violation (Licensing):
MIN.1 - Targeted Malware Attacks:	x	x	x	x	x	x	x	x		
MIN.2 - Targeted Ransomware Attacks:	x	x	x	x	x	x	x	x		
MIN.3 - Target Phishing/Spam Attacks:	x	x	x	x	x	x	x	x		
MIN.4 - Target Attacks to Information Systems:	x	x	x	x	x	x	x	x		
MIN.5 - Non-targeted Malware Attacks:	x	x	x	x	x	x	x	x		
MIN.6 - Targeted Ransomware Attacks:	x	x	x	x	x	x	x	x		
MIN.7 - Non-Target Phishing/Spam Attacks:		x	x	x	x	x	x	x		
IN.8 - Non-Target Attacks to Information Systen	x	x	x	x	x	x	x	x		
MIN.9 - DOS Attacks:	x									
MIN.10 - Social Engineering Attacks:				x	x	x				
MIN.11 - Targeted Attacks by vendors:	x	x	x	x	x	x	x	x		
MIN.12 - Lock-in (only one Vendor - xxx):										
MIN.13 - Error during development phase:	x	x	x	x	x	x	x	x		
MIN.14 - Error during testing / release:	x	x	x	x	x	x	x	x		
I.15 - Error during operation by Business Operat	x	x	x	x	x	x	x	x		
MIN.16 - Error during operation by SA:	x	x	x	x	x	x	x	x		
MIN.17 - Central IT systems hw failure:	x	x	x				x	x		
MIN.18 - Auxiliary systems Failure:	x	x	x							
MIN.19 - Telecommunication line failure:	x									
MIN.20 - Theft of user devices:		x	x	x	x	x	x	x		
MIN.21 - Physical Intrusions:	x	x	x	x	x	x				
MIN.22 - Environmental events:	x	x	x				x	x		
MIN.23 - Compliance Violation (Privacy):									x	
MIN.24 - Compliance Violation (Licensing):										x
MIN.25 - Technological obsolescence:	x	x	x	x	x	x	x	x		

Figure 11: Threat-Consequences couples

The campaign life cycle will be described later in this chapter.

7.1.1.6. Questionnaire

Two types of questionnaires exist: Application IT Assessments and Control Assessments.

1. Application IT Assessment

An Application IT Assessment is created every time a campaign includes an IT Application for the first time in a quarter.

This kind of questionnaire is characterized by an owner, depending on the domain of the application, and a review status field which indicates if its responsible user has evaluated it.

The body of the questionnaire is filled with questions about the risk context factors, threats and consequences, as shown in Figure 12.

The answers to the questionnaires affect the risk calculations.

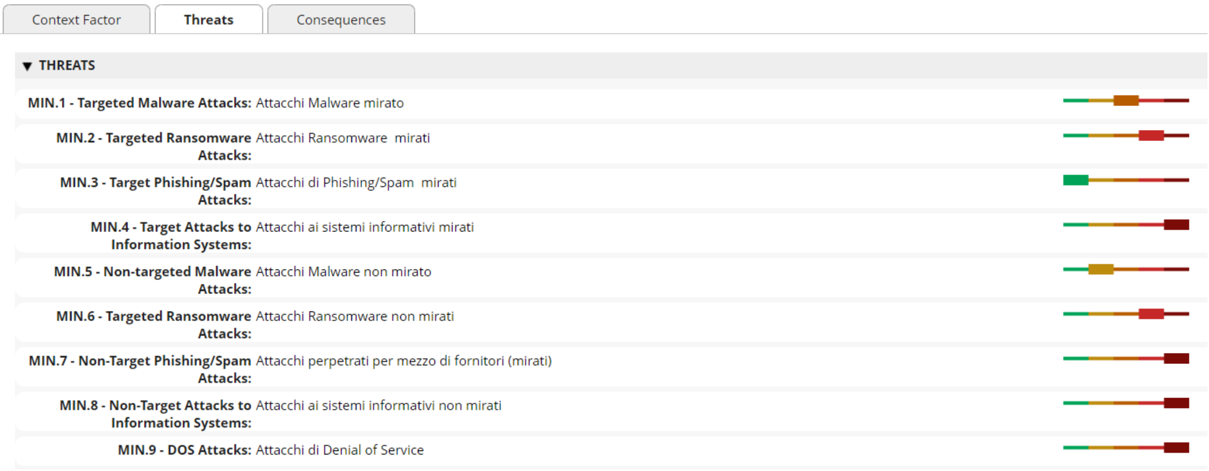
2. Control Assessment

Control assessments also present a review status field equivalent to application questionnaires, but they are much simpler and only asks the application *Custodian* to evaluate the maturity of the control.

The control maturity also affects risk calculations.

7.1.1.7. Remediation Plan

Remediation Plans are still in the design phase but, as of today, they will act as remediation actions: there will not be this distinction.



▼ THREATS

MIN.1 - Targeted Malware Attacks: Attacchi Malware mirato

MIN.2 - Targeted Ransomware Attacks: Attacchi Ransomware mirati

MIN.3 - Target Phishing/Spam Attacks: Attacchi di Phishing/Spam mirati

MIN.4 - Target Attacks to Information Systems: Attacchi ai sistemi informativi mirati

MIN.5 - Non-targeted Malware Attacks: Attacchi Malware non mirato

MIN.6 - Targeted Ransomware Attacks: Attacchi Ransomware non mirati

MIN.7 - Non-Target Phishing/Spam Attacks: Attacchi perpetrati per mezzo di fornitori (mirati)

MIN.8 - Non-Target Attacks to Information Systems: Attacchi ai sistemi informativi non mirati

MIN.9 - DOS Attacks: Attacchi di Denial of Service

Figure 12: Questionnaire example

Remediation Plans will represent the actions to be actuated to mitigate the risk and will be the additional input needed to calculate the residual risk.

7.1.2. Campaign life cycle

As briefly mentioned before, the IT Risk Administrator creates and launches campaigns. As shown in Figure 13, a campaign starts its life cycle with "New" as its status. After the admin has added the IT applications to the campaign scope and has launched the campaign, the status changes into "In progress".

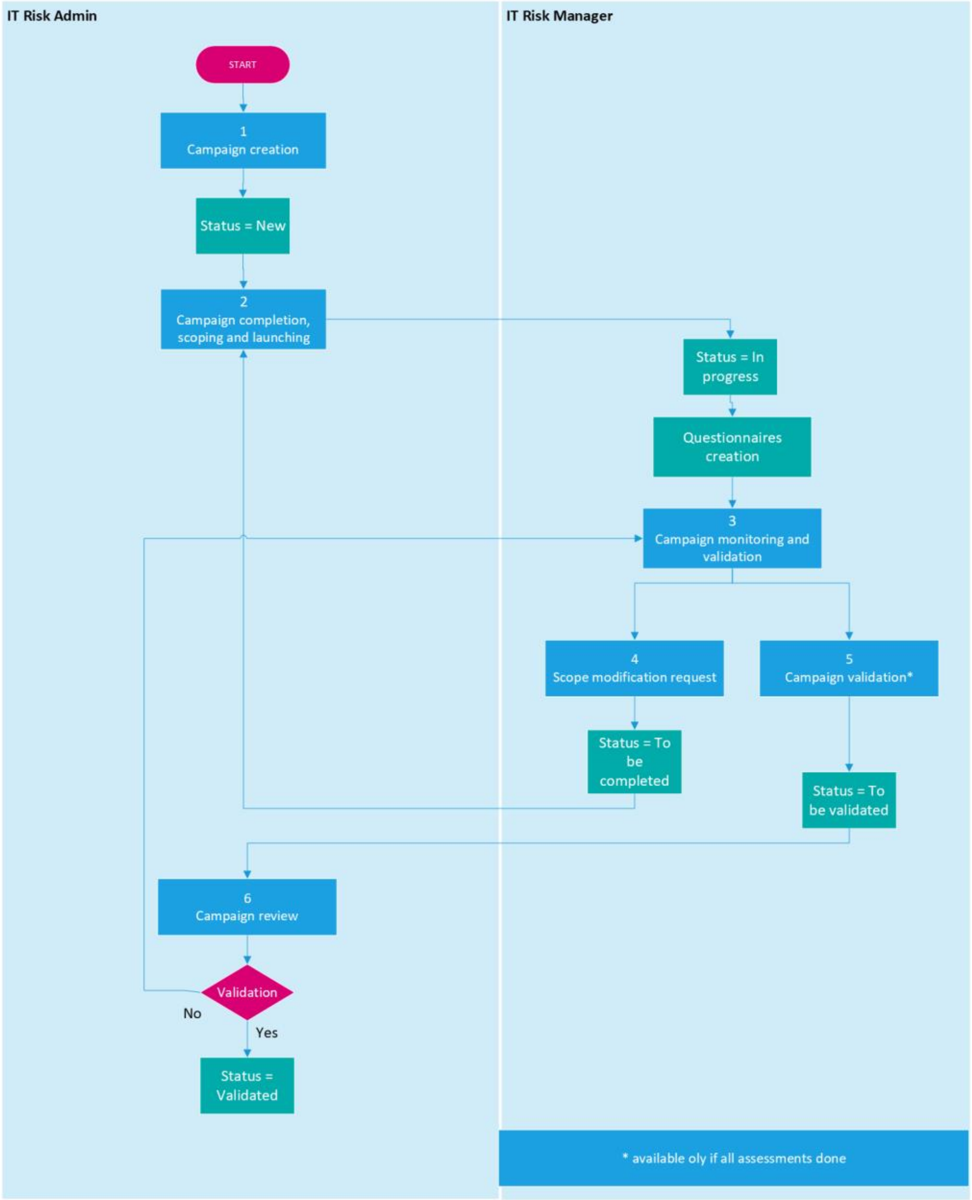


Figure 13: Campaign life cycle

At this point, the campaign manager assigned to the task receives a notification that reminds him to review the campaign questionnaire. At the same time, components' custodians review the control assessments.

The campaign manager can ask the administrator for the rescoping of the campaign (status "to be completed") or propose to validate the campaign ("to be validated").

In both cases, control returns to the administrator who, in the first case, can relaunch the campaign or, in the second one, validate it or not.

In case of rejection, the campaign goes back to "in progress state", where the administrator will ask the custodians to review the evaluations.

In case of validation, if all the questionnaires are completed and in "approved" status, the campaign is closed and put into "validated" status.

7.1.3. Risk calculation process

In the following pages I will briefly explain the risk calculation process implemented on Archer during the project according to the risk model, and which formed a significant part of my engagement in the project.

As explained in the preceding chapter, there are three calculations to be performed:

- IT Risk Calculation: Inherent Risk based on the Application IT questionnaire
- IT Risk Calculation: Effective Risk based on the control results and the Inherent Risk calculated
- IT Risk Calculation: Residual Risk based on the remediation plan, the control results and the Inherent Risk.

7.1.3.1. IT Risk: Inherent Calculation

Step 1 (Figure 14): the user is asked about Context Factors, Threats and Consequences inside a questionnaire. The last values of each answer of the questionnaire are automatically replicated inside the application IT.

The user can see all the history of evaluation of the IT application. When a new assessment of the questionnaire is created, the last validated responses to context factors, threats and consequences are copied and can be modified. The user, therefore, only goes to express the changes (delta logic), leaving unchanged the information that has not changed over time.

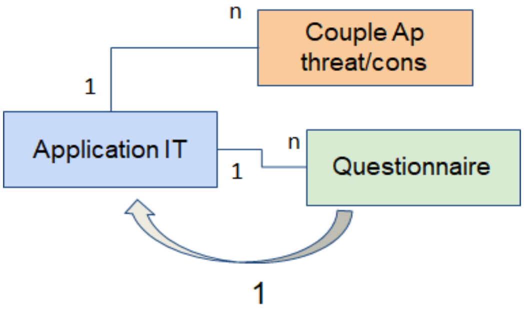


Figure 14: Inherent risk calculation step 1

Step 2: the answers are used to calculate Inherent risk inside the related couples threat/consequence.

For each option possible in the answers, a value is provided to be used for the calculation.

The probability of each couple threat/consequence is calculated based on the results of the context factors and the threats using an appropriate matrix.

The impact of each couple threat/consequence is calculated based on the results corresponding consequence.

The final risk level of each couple is calculated by the multiplication of the impact with the probability.

Step 3 (Figure 15): individual Inherent risk score at threat/consequence level is aggregated at Application IT Level.

For each threat, consequence and globally, the aggregation used is the MAX for the impact and the AVERAGE for the probability.

In additional, globally, the aggregation is done using the MAX for the impact and probability and then the MIN for the impact and the probability.

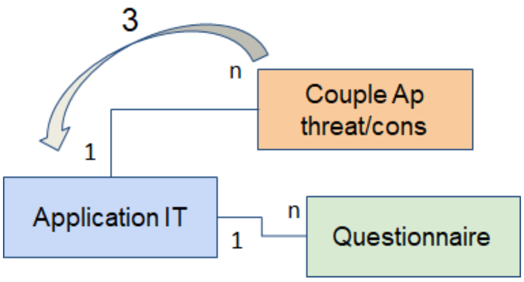


Figure 15: Inherent risk calculation step 3

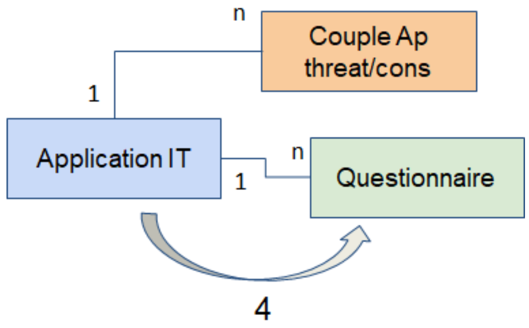


Figure 16: Inherent risk calculation step 4

Step 4 (Figure 16): all calculations done at the application IT level are historized into the questionnaire.

7.1.3.2. IT Risk: Effective Calculation

Step 1 (Figure 17): the user is asked about control maturity level through the control questionnaire created for each control. The last values of each answer of the questionnaire are automatically replicated inside the corresponding control.

The user can see all the history of evaluation of the control. When a new assessment of the questionnaire is created, the last validated responses (maturity and comment) are copied and can be modified. The user, therefore, only goes to express the changes (delta logic), leaving unchanged the information that has not changed over time.

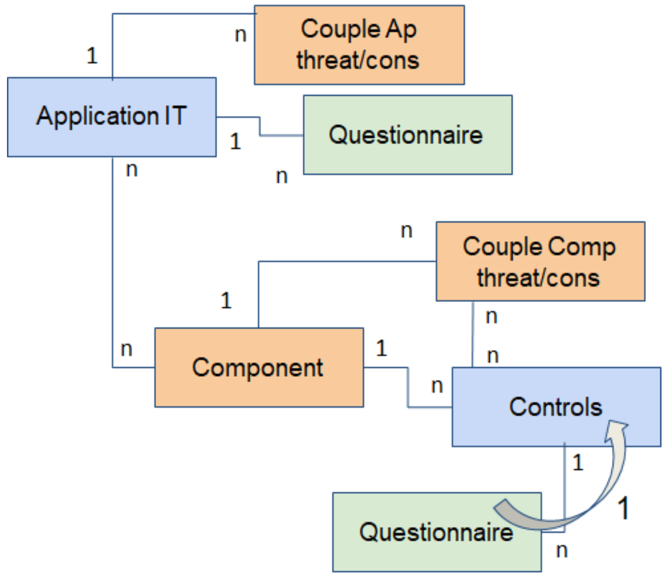


Figure 17: Effective risk calculation step 1

Step 2 (Figure 18): the mitigation factor for each couple (component related) threat/consequence are calculated inside the couples with AVERAGE aggregation of maturity level of the related controls using the weight of each control and the identification if a control has an effect on the impact, the probability or both.

It is important to remark that the link between the couples threat/consequence and the controls is automatically determined based on:

- the component shared
- the common threat
- the common consequence.

Step 3 (Figure 19): the mitigation factor for each couple (application related) threat/consequence are calculated inside the couples with AVERAGE aggregation of mitigation factor of corresponding couples comp threat/cons using the weight of couple comp threat/cons.

It is important to remark that the link between the couples (component related) threat/consequence and the couple (application related) threat/consequence is automatically determined based on:

- the application IT shared
- the common threat
- the common consequence.

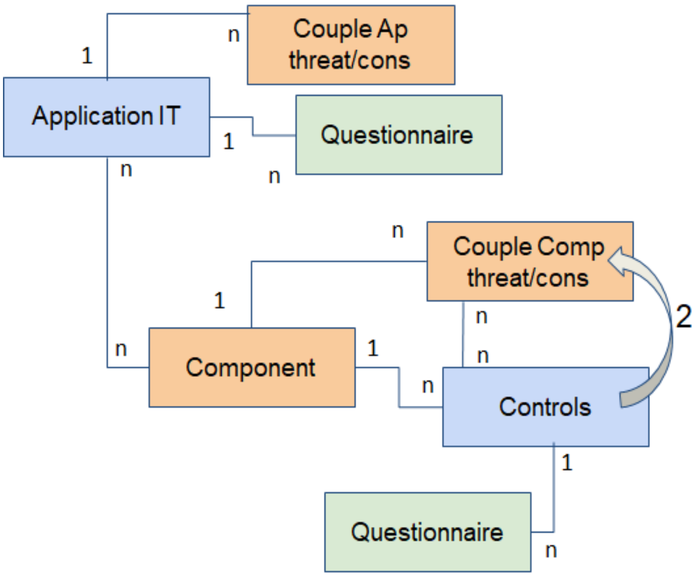


Figure 18: Effective risk calculation step 2

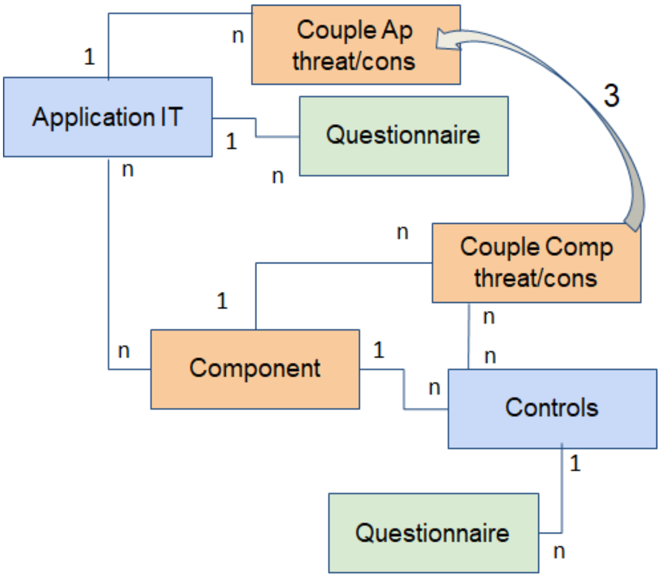


Figure 19: Effective risk calculation step 3

Step 4 (Figure 20): individual effective risk score at threat/consequence level is aggregated at Application IT Level. The same approach is followed as for the Inherent risk.

For each threat, consequence and globally, the aggregation used is the MAX for the impact and the AVERAGE for the probability.

In additional, globally, the aggregation is done using the MAX for the impact and probability and then the MIN for the impact and the probability.

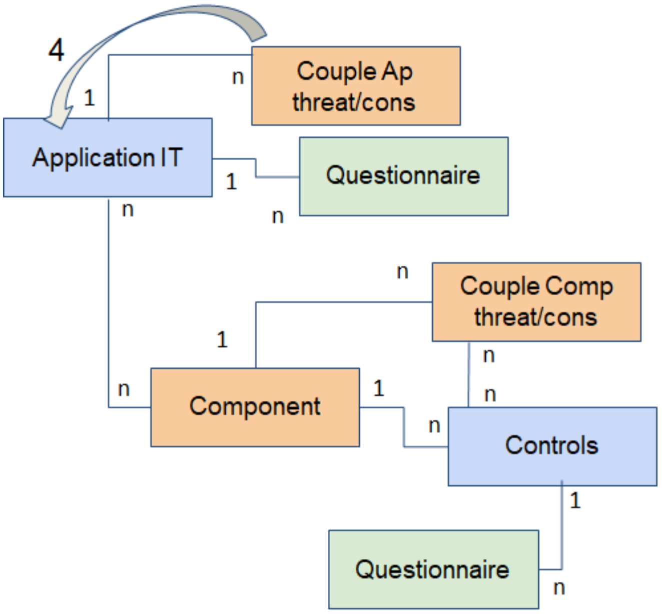


Figure 20: Effective risk calculation step 4

Step 5: all calculations done at the application IT level are historized into the questionnaire. The same approach is followed as for the Inherent risk.

7.1.3.3. IT Risk: Residual Calculation

The procedure for evaluating Residual IT Risk is virtually the same as the one for Effective IT Risk.

The only difference is we are taking in account the value, if existing, in the remediation plan linked to the controls in priority of the last assessment of the controls.

The rest of the calculation is exactly the same.

7.1.3.4. IT Risk: calculation process indicators

The following indicators support the Operational Referent in monitoring and analyzing the quality of the data.

The Operational Referent is interested in understanding the quality of the information collected (% of responses with answer “I don’t know”) and the average maturity of the answers collected (the IT security status of a component). Usually, The Operational Referent analyses data by Custodian but it could also analyze data by Component.

Indicators on Component implemented during the project:

- Indicator.1 average maturity of controls
- Indicator.2 % of controls with answer "I don't know".

Indicators on Custodian implemented during the project:

- - Indicator.3 average maturity of controls
- - Indicator.4 % of controls with answer "I don't know".

All these indicators will be calculated in report based on the controls results and filter by custodian (user) or component.

7.2. Building

After the design phase was completed through the approval of detailed requirements, the building activities began, which massively involved consulting personnel, both process experts and Archer experts, and to a much lesser extent the company's personnel, who primarily played the role of information providers and validators of proposed solutions, as experts of the process being modelled. A small group of referents from the company were trained to use the system at the end of the building phase, with specific theoretical and practical training sessions, in order to actively participate in the subsequent testing phase.

The building phase activities that I was particularly involved in are:

- System configuration

- Training of key personnel in the use of reporting.

As previously mentioned, the functional richness and flexibility of the software often allowed the system itself to be used, rather than ad hoc prepared documentation, in order to validate the configuration activities carried out. This allowed users to have a realistic (look and feel) view of the system and consultants to quickly modify solutions to adapt to the needs that emerged during validation activities.

7.2.1. System configuration

The heaviest load of work in the whole project was undoubtedly the platform configuration. Personally, I wasn't involved in the initial configuration since a team of commissioned Archer professionals was entrusted with that part, but, soon after the first "draft" release in the development environment, the HSPI team, including me, took an active role in refining the work done and implementing the second set of features.

The tools that are used the most to configure archer are the application builder and the data feeds manager. Other aspects that saw our intervention were the notification system and the dashboards.

7.2.1.1. Application builder

This is the core aspect of the archer implementation. Here applications are built by creating new fields or modifying existing ones and implementing all the relations between said fields.

The application builder presents itself with four main tabs:

- Properties
- Designer
- Workflow
- Calculations.

7.2.1.1.1. Properties

The properties tab allows the configuration of the application in general, by setting parameters such as the application name or the default language, but most importantly it's the section where the opening screen of the application is configured.

The opening screen of an application is always a report in table form that shows the instances of the application. For example, in the case of the Risk Register application, the opening screen report shows all the risks for the different solution areas. The interface allows the user to filter out, for example, the operational, compliance and Legge 231 records to only show IT risks.

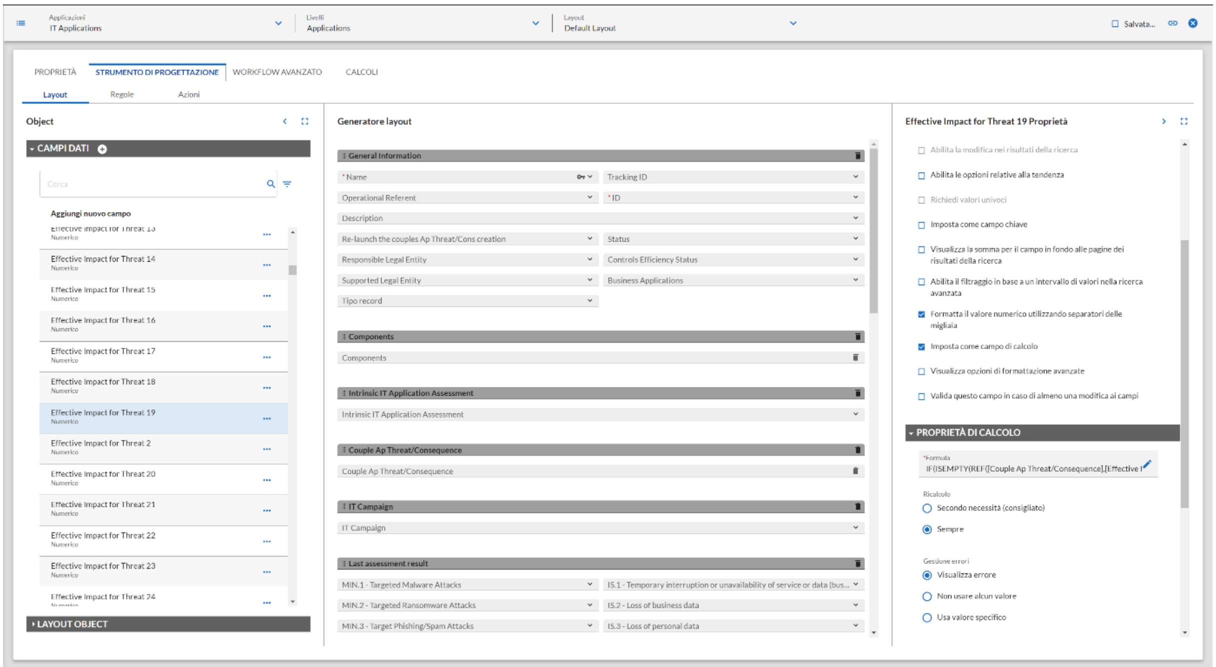
The report can be configured to show only specific fields of the application and order the fields according to a certain criterion.

7.2.1.1.2. Designer

Designer tab (Figure 21) is the core part of the application builder. It consists of three sub-tabs:

- Layout
- Rules
- Actions.

The layout tab is where the fields are managed. From this tab fields can be added to the visualization inside of an application instance. Moreover, this is where fields properties are set. For example, the definition of a field as a value list or as a calculated field happens here. For calculated fields, this is also the place where formulas are defined. The formulas (Figure 22) are written in a pseudo-code formal language that includes basic mathematical operators and IF clauses. Sometimes the language, despite the simplicity of use, can be limiting by the fact that it does not support the use of variables.



Effective Impact for Threat 13 Numerico
Effective Impact for Threat 14 Numerico
Effective Impact for Threat 15 Numerico
Effective Impact for Threat 16 Numerico
Effective Impact for Threat 17 Numerico
Effective Impact for Threat 18 Numerico
Effective Impact for Threat 19 Numerico
Effective Impact for Threat 2 Numerico
Effective Impact for Threat 20 Numerico
Effective Impact for Threat 21 Numerico
Effective Impact for Threat 22 Numerico
Effective Impact for Threat 23 Numerico
Effective Impact for Threat 24 Numerico

General Information
- *Name | Tracking ID
- Operational Referent | *ID
- Description
- Re-launch the couples Ap Threat/Cons creation | Status
- Responsible Legal Entity | Controls Efficiency Status
- Supported Legal Entity | Business Applications
- Tipo record

Components
- Components

Intrinsic IT Application Assessment
- Intrinsic IT Application Assessment

Couple Ap Threat/Consequence
- Couple Ap Threat/Consequence

IT Campaign
- IT Campaign

Last assessment result
- MIN.1 - Targeted Malware Attacks | IS.1 - Temporary interruption or unavailability of service or data (bus...
- MIN.2 - Targeted Ransomware Attacks | IS.2 - Loss of business data
- MIN.3 - Target Phishing/Spam Attacks | IS.3 - Loss of personal data

Effective Impact for Threat 19 Proprietà

□ Abilita la modifica nei risultati della ricerca
□ Abilita le opzioni relative alla tendenza
□ Richiedi valori univoci
□ Imposta come campo chiave
□ Visualizza la somma per il campo in fondo alle pagine dei risultati della ricerca
□ Abilita il filtraggio in base a un intervallo di valori nella ricerca avanzata
☑ Formatta il valore numerico utilizzando separatori delle migliaia
☑ Imposta come campo di calcolo
□ Visualizza opzioni di formattazione avanzate
□ Valida questo campo in caso di almeno una modifica ai campi

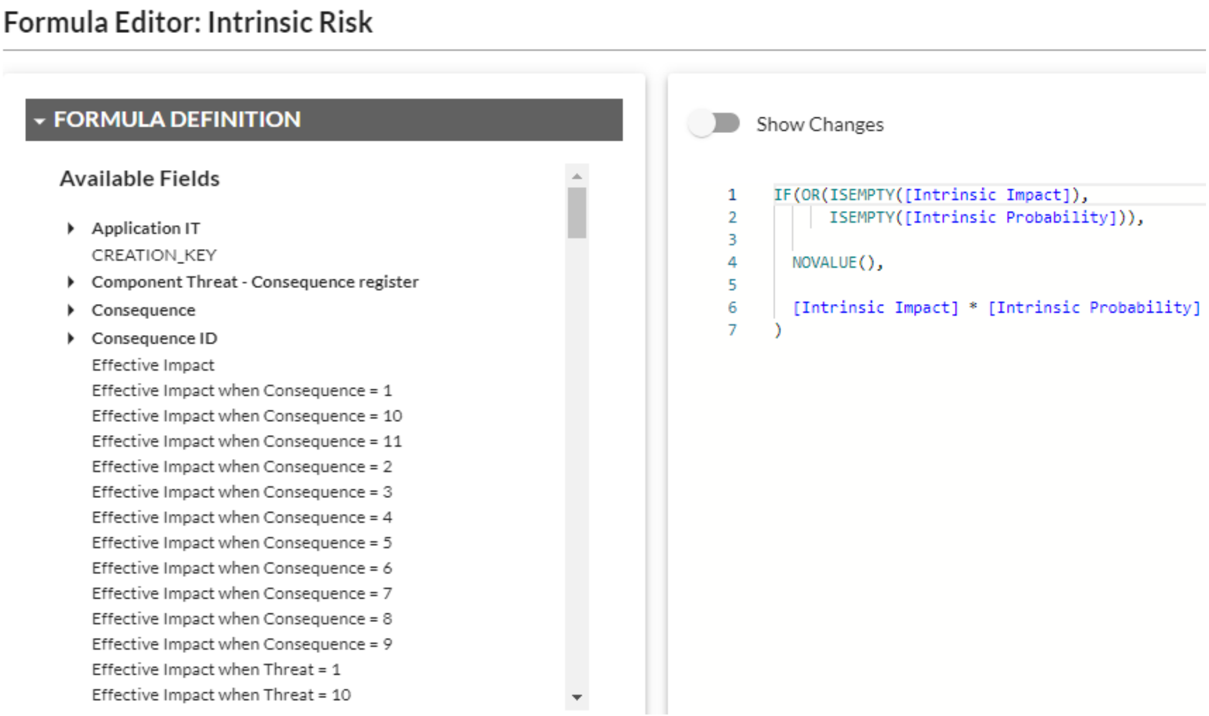
PROPRIETÀ DI CALCOLO

*Formula: IF(ISEMPTY(REF([Couple Ap Threat/Consequence],[Effective I

Ricalcolo
○ Secondo necessità (consigliato)
● Sempre

Gestione errori
● Visualizza errore
○ Non usare alcun valore
○ Usa valore specifico

Figure 21: Application builder interface, layout designer tab



Formula Editor: Intrinsic Risk

▾ FORMULA DEFINITION

Available Fields

- ▸ Application IT
- CREATION_KEY
- ▸ Component Threat - Consequence register
- ▸ Consequence
- ▸ Consequence ID
- Effective Impact
- Effective Impact when Consequence = 1
- Effective Impact when Consequence = 10
- Effective Impact when Consequence = 11
- Effective Impact when Consequence = 2
- Effective Impact when Consequence = 3
- Effective Impact when Consequence = 4
- Effective Impact when Consequence = 5
- Effective Impact when Consequence = 6
- Effective Impact when Consequence = 7
- Effective Impact when Consequence = 8
- Effective Impact when Consequence = 9
- Effective Impact when Threat = 1
- Effective Impact when Threat = 10

```
IF(OR(ISEMPTY([Intrinsic Impact]),
      ISEMPTY([Intrinsic Probability])),

  NOVALUE(),

  [Intrinsic Impact] * [Intrinsic Probability]
)
```

Figure 22:Calculated field formula

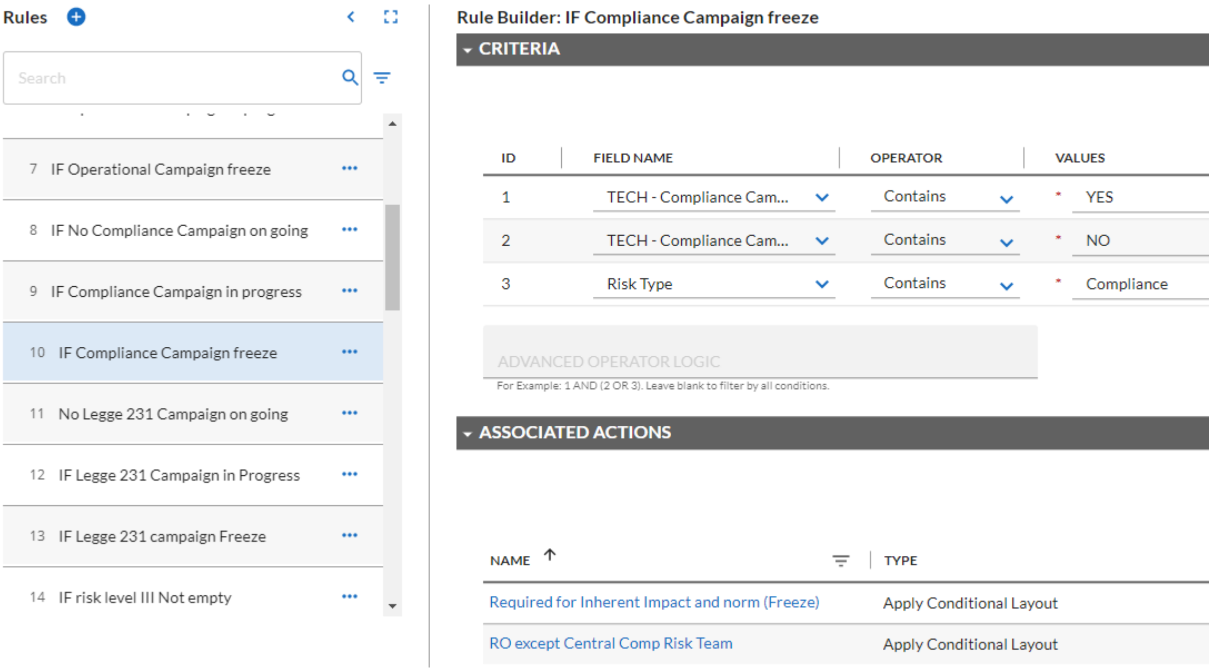
Rules and actions defines what a user sees and can interact with.

Rules determine whether a field meets a criterion: a certain field is confronted against a value through an operator depending on the nature of the field. If the different criteria are satisfied, according to the operator logic that connects them, then the actions associated to the rule are applied.

An action can apply a certain conditional layout or can intervene on the items of a value list. In any case, an action can be implemented for specific users or groups of user, by including or excluding them from the effects of the action.

A typical example, in our implementation of Archer for the customer company, is the set of rules and actions that hide fields specific of a solution area to the users of other solution areas with whom the application is in common.

In Figure 23 and Figure 24 are depicted two examples, one of a rule and another one of an action.



Rules

7	IF Operational Campaign freeze
8	IF No Compliance Campaign on going
9	IF Compliance Campaign in progress
10	IF Compliance Campaign freeze
11	No Legge 231 Campaign on going
12	IF Legge 231 Campaign in Progress
13	IF Legge 231 campaign Freeze
14	IF risk level III Not empty

Rule Builder: IF Compliance Campaign freeze

CRITERIA

ID	FIELD NAME	OPERATOR	VALUES
1	TECH - Compliance Cam...	Contains	* YES
2	TECH - Compliance Cam...	Contains	* NO
3	Risk Type	Contains	* Compliance

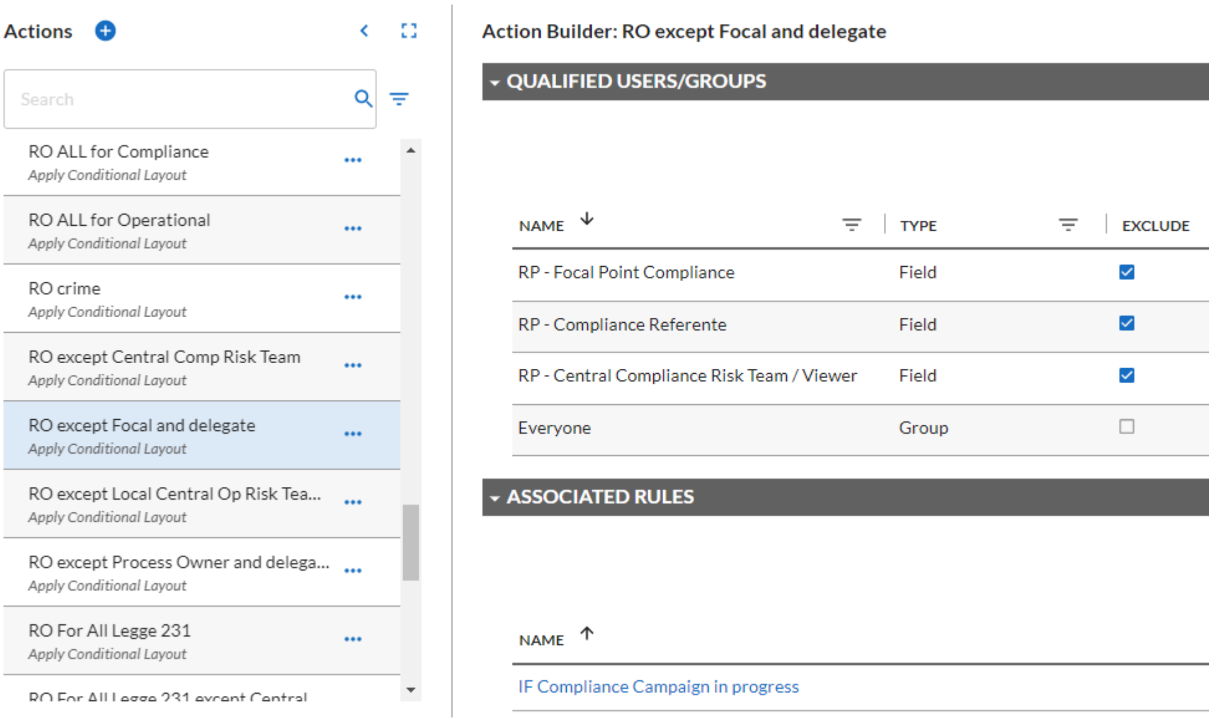
ADVANCED OPERATOR LOGIC

For Example: 1 AND (2 OR 3). Leave blank to filter by all conditions.

ASSOCIATED ACTIONS

NAME	TYPE
Required for Inherent Impact and norm (Freeze)	Apply Conditional Layout
RO except Central Comp Risk Team	Apply Conditional Layout

Figure 23: Example of rule



Actions

RO ALL for Compliance *Apply Conditional Layout*
RO ALL for Operational *Apply Conditional Layout*
RO crime *Apply Conditional Layout*
RO except Central Comp Risk Team *Apply Conditional Layout*
RO except Focal and delegate *Apply Conditional Layout*
RO except Local Central Op Risk Tea... *Apply Conditional Layout*
RO except Process Owner and delega... *Apply Conditional Layout*
RO For All Legge 231 *Apply Conditional Layout*
RO For All Legge 231 except Central

Action Builder: RO except Focal and delegate

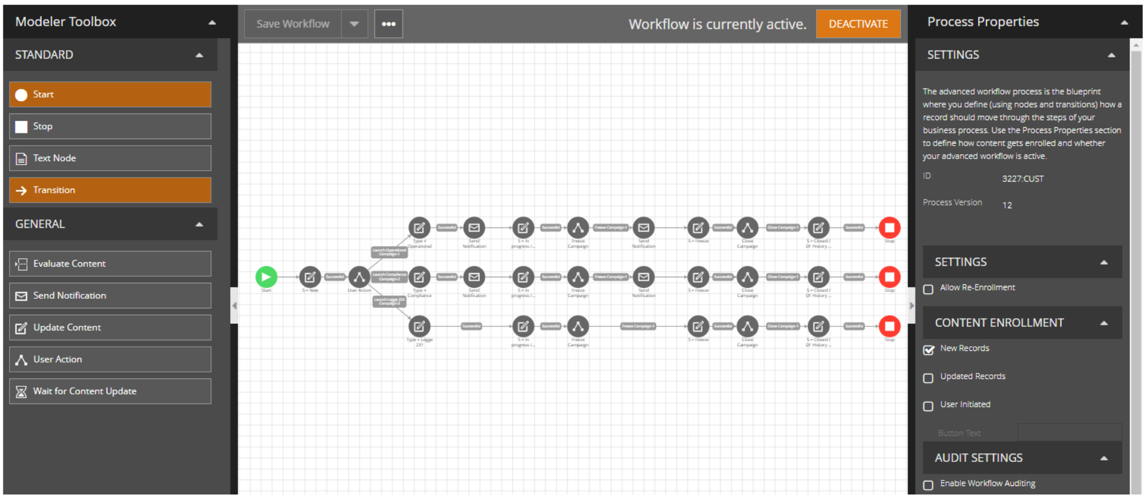
QUALIFIED USERS/GROUPS

NAME	TYPE	EXCLUDE
RP - Focal Point Compliance	Field	☑
RP - Compliance Referente	Field	☑
RP - Central Compliance Risk Team / Viewer	Field	☑
Everyone	Group	☐

ASSOCIATED RULES

NAME
IF Compliance Campaign in progress

Figure 24: Example of action



The advanced workflow process is the blueprint where you define (using nodes and transitions) how a record should move through the steps of your business process. Use the Process Properties section to define how content gets enrolled and whether your advanced workflow is active.

ID 3227:CUST

Process Version 12

SETTINGS

□ Allow Re-Enrollment

CONTENT ENROLLMENT

☑ New Records

□ Updated Records

□ User Initiated

Button Text

AUDIT SETTINGS

□ Enable Workflow Auditing

Figure 25: Workflow modeler example

7.2.1.1.3. *Workflow*

The workflow modeler toolbox (Figure 25) is a graphical design tool to implement the desired interaction of users with the application. Its main purpose is to differentiate the roles and consequent actions at each step of the application process flow.

An example of our implementation is the workflow of the IT campaigns. Depending on the stage of the campaign, different actors are involved:

- The IT Risk Admin creates a campaign, the workflow sends a notification and enables to the IT Risk Manager to take control of the campaign
- The IT risk manager add IT applications and launches the campaign and the launch action triggers the workflow to launch in turn data feeds that generates questionnaires
- The custodians are informed and their questionnaires evaluation job begins.

The passages in the workflow can be subject to rules too. Certain actions can be enabled or forbidden by evaluating fields.

7.2.1.1.4. *Calculations*

The calculation tab simply determines the order in which the fields are calculated and the recalculation routine, that can be scheduled or launched manually.

7.2.1.2. Data feeds

Data feeds use the information contained in reports populated by the workflow to run automatic operations, such as the creation of questionnaires for an IT risk campaign.

They are scheduled to run every few minutes and when they find that the users actions triggered the workflow to set some report fields to certain values, they produce some outputs.

For example, in the case of the IT risk campaign, when a campaign is launched, the data feeds verify if the campaign is the first of a quarter by looking at a calculated field and if there are questionnaires to create by checking a field set by the campaign launch action in the workflow.

We had to go through a lot of trial and error in order to finally achieve the configuration of data feeds and workflow indicator fields that implemented the correct creation of questionnaires. This was particularly tricky since new questionnaires need to be precompiled with previous questionnaires information and only need to be created for the first campaign of a certain quarter that includes in its scope certain IT applications.

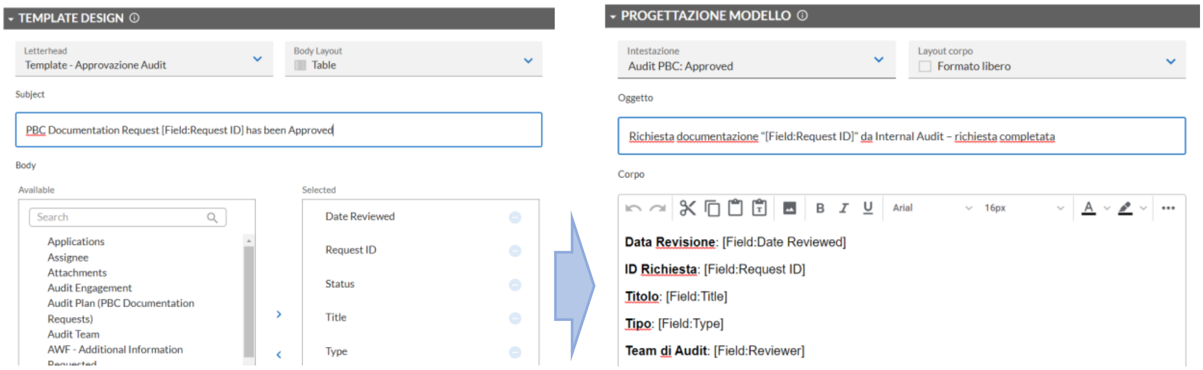
7.2.1.3. Notifications

Default notification letterheads are included in the Archer suite, however we had to refine the templates and the single application notifications in order to adapt them to the customer's needs (Figure 26).

One of the biggest issues was that the templates were in English and the translation files do not include notification translations. For this reason, we had to rebuild, nearly from scratch, the templates to present the text first in Italian and then in the languages of the foreign companies. This was obtained by substituting the preset tables with free text accompanied by fields references.

7.2.2. Training of the referents on the use of reporting

It was agreed that the consulting team should train the referents of the various areas on how to create reports, charts and export the data. All should have taken place during a couple of workshops per area. Actually, we ended up creating most of the reports that were meant to be made by the company with our support.



TEMPLATE DESIGN

Letterhead: Template - Approvazione Audit

Body Layout: Table

Subject: PBC Documentation Request [Field:Request ID] has been Approved

Body

Available: Applications, Assignee, Attachments, Audit Engagement, Audit Plan (PBC Documentation Requests), Audit Team, AWF - Additional Information Requested

Selected: Date Reviewed, Request ID, Status, Title, Type

PROGETTAZIONE MODELLO

Intestazione: Audit PBC: Approved

Layout corpo: Formato libero

Oggetto: Richiesta documentazione "[Field:Request ID]" da Internal Audit – richiesta completata

Corpo

Data Revisione: [Field:Date Reviewed]

ID Richiesta: [Field:Request ID]

Titolo: [Field:Title]

Tipo: [Field:Type]

Team di Audit: [Field:Reviewer]

Figure 26: Notification template change

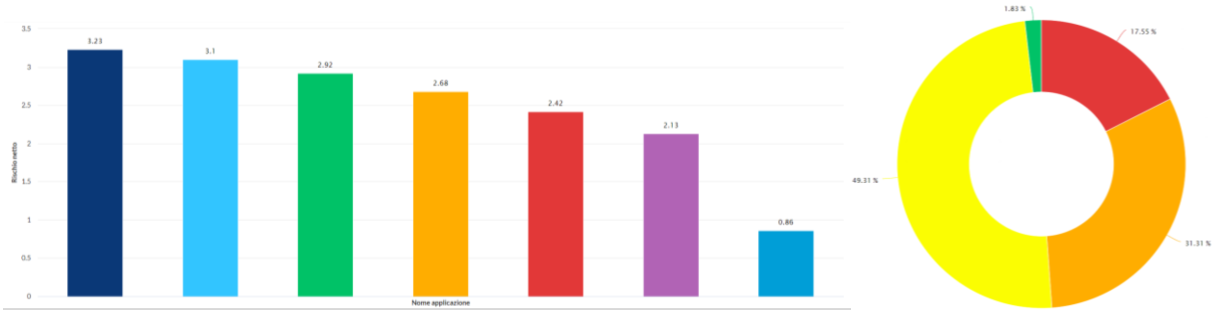


Figure 27: Examples of charts (anonymized)

I was given the task of preparing the reports and presenting them to the teams of the different areas. We started with operational risk and compliance and then loss data collection followed. After that it was the turn of IT risk and finally internal audit.

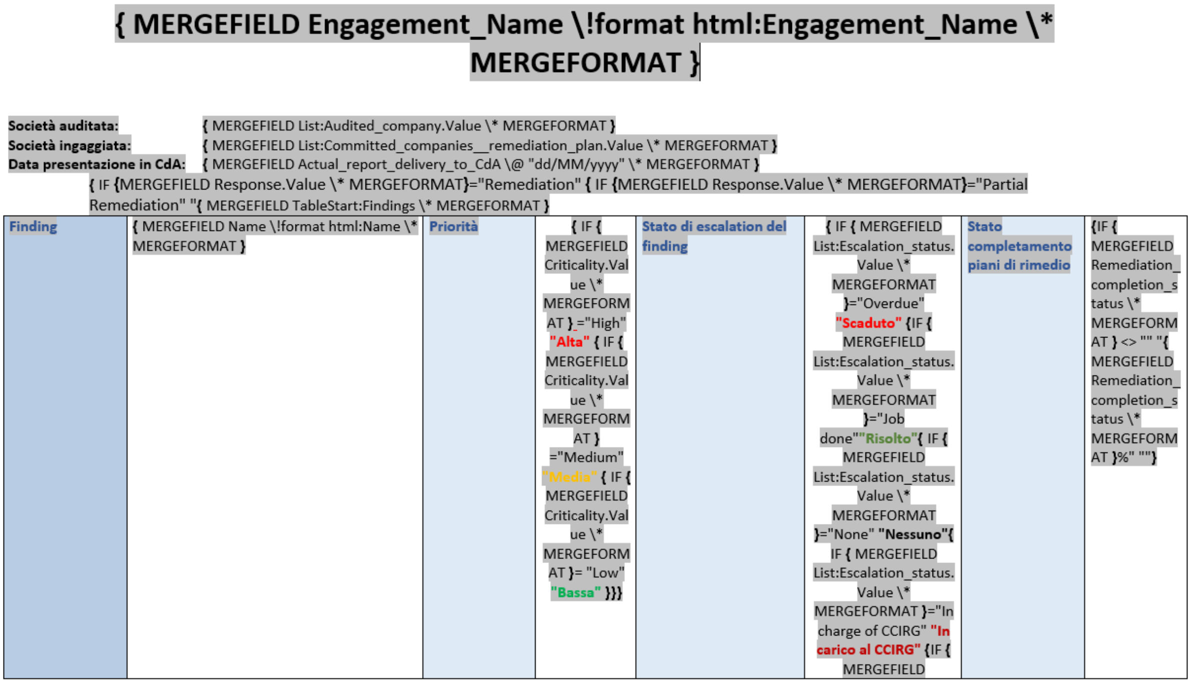
The reports that the company wanted to be built were previously agreed on, since this also affected some design choices. For example, reports regarding historical data required some fields to be added to applications meant to keep the data from previous years frozen in time, even when the present values in the fields change.

The reports included tables, histograms, donuts, Pareto's and mail merge templates (Figure 27).

Unfortunately, the Pareto's charts in Archer always consider the data you feed them as the totality of data on which to plot the chart on. This means, for instance, that you cannot have a Pareto's chart that shows the percentage of a certain quantity, such as total risk, mapped by the first X processes. If you filter the data to only show the first X processes in the Pareto's chart, Archer will still plot the Pareto's curve from 0% to 100%, and not to the percentage mapped by the first X processes. To avoid this problem, the only workaround that was found is to prepare the reports that should include the Pareto's in table form and then extract the data to process it in another tool such as Excel.

Screenshots of the reports were collected in Power Point slides for the different solution areas in preparation of the workshops.

After the preparation of the reports, we had workshops with the referents of the different solution areas, in which the reports were presented and slightly adjusted to better fit the company's needs. During these sessions we created the remaining reports that were not made before the workshops, either because we needed more detailed information from the customers or because they were not present in the previously agreed report list.



{ MERGEFIELD Engagement_Name \!format html:Engagement_Name * MERGEFORMAT }

Società auditata: { MERGEFIELD List:Audited_company.Value * MERGEFORMAT }
Società ingaggiata: { MERGEFIELD List:Committed_companies__remediation_plan.Value * MERGEFORMAT }
Data presentazione in CdA: { MERGEFIELD Actual_report_delivery_to_CdA \@ "dd/MM/yyyy" * MERGEFORMAT }
{ IF {MERGEFIELD Response.Value * MERGEFORMAT}="Remediation" { IF {MERGEFIELD Response.Value * MERGEFORMAT}="Partial Remediation" "{ MERGEFIELD TableStart:Findings * MERGEFORMAT }

Finding	{ MERGEFIELD Name \!format html:Name * MERGEFORMAT }	Priorità	{ IF { MERGEFIELD Criticality.Value * MERGEFORMAT } ="High" "Alta" { IF { MERGEFIELD Criticality.Value * MERGEFORMAT } ="Medium" "Media" { IF { MERGEFIELD Criticality.Value * MERGEFORMAT }= "Low" "Bassa" }}}	Stato di escalation del finding	{ IF { MERGEFIELD List:Escalation_status.Value * MERGEFORMAT }="Overdue" "Scaduto" {IF { MERGEFIELD List:Escalation_status.Value * MERGEFORMAT }="Job done""Risolto"{ IF { MERGEFIELD List:Escalation_status.Value * MERGEFORMAT }="None" "Nessuno"{ IF { MERGEFIELD List:Escalation_status.Value * MERGEFORMAT }="In charge of CCIRG" "In carico al CCIRG" {IF { MERGEFIELD	Stato completamento piani di rimedio	{IF { MERGEFIELD Remediation_completion_status * MERGEFORMAT } <> "" "{ MERGEFIELD Remediation_completion_status * MERGEFORMAT }%" ""}

Figure 28: Example of mail merge template

For internal audit, in particular, the company asked us to create Microsoft Word's mail merge templates (Figure 28) that could be used to present, in a tidy way, the audit results to the board. This function, that uses standard Word functionalities, because of a patch in Archer, forced us to rebuild the templates. In fact, before the patch, Archer, because of a bug, populated mail merge fields with English only content, ignoring the translations in Italian and Spanish. Because of this issue, the templates were configured to bring in data in English and convert it in Italian through IF clauses. During the testing of the patch, we verified that the update solved the bug, but nonetheless, we had to reconfigure all the templates to manage data in Italian.

Following the workshops, because of the large variety of fields present in the Archer implementation, we prepared catalogues of fields useful for creating further reports, one for each solution area. The catalogues grouped the fields by application and added a few notes when needed.

7.3. Test

During the building phase, the working team took care of performing tests in the development environment, both local (on the single functionality just developed) and global, on the processes supported by the different functionalities and on the system as a whole, using test data.

This allows to evaluate the adherence of what has been developed with the requirements formalized in the requirements analysis.

These tests were carried out by the consulting personnel, with the involvement of company personnel when necessary.

It should be noted that these are not the classic tests on ad hoc developed software, as the implementation of Archer does not require software development. Therefore, a specific testing methodology has been adopted for the testing of the product configuration, not for its development.

Once the tests were successfully completed in the development environment, comprehensive tests were carried out with the users to verify whether the developed functionalities actually solve the problems for which they were implemented.

This type of test (UAT) was conducted in a dedicated environment, using data that closely approximates what is actually used in production.

The execution of the tests involved various activities, such as:

- populating the UAT environment (ETL)
- conducting tests and formalizing results
- managing bug fixing requests in case of malfunctions
- managing change requests if the adopted solution is not adequate for the company's needs.

7.3.1. ETL

In order to populate the UAT environment with actual data, before the implementation of the automatic feeder of data coming from Aris, we had to do some manual imports. To do so, data needed to be converted from the Aris template to a structure eligible to be uploaded into Archer, according to the specific configuration implemented for the company.

This implied following the various stages of the ETL process:

1. Data extraction
2. Data validation
3. Data transformation
4. Data import.

The data extraction was carried out by the company members, who extracted the data and provided it to the consulting team.

7.3.1.1. Data validation

Even the data that came from a structured environment such as that of Aris was not always ready to be uploaded into the GRC for different reasons:

- Missing data: some records were missing required information that would have caused the import to fail. Some fields were configured as strictly mandatory in the Archer implementation while in systems previously adopted nothing forced the obligatoriness of that data
- Duplicated data: some records had clones that were not needed and, though, redundant. In some cases, this would have simply burdened the system, in some other cases this would have caused malfunctions
- Unwanted data: there were cases when records like risks or questionnaires, related, for example, to abandoned processes or dismissed applications, were provided for the import, but they would have been useless since they missed the father, and so were no to be uploaded.

We, as the consulting team, managed to fix the inconsistencies and get the data ready for transformation by a continuous confrontation with the data providers from the company.

7.3.1.2. Data transformation

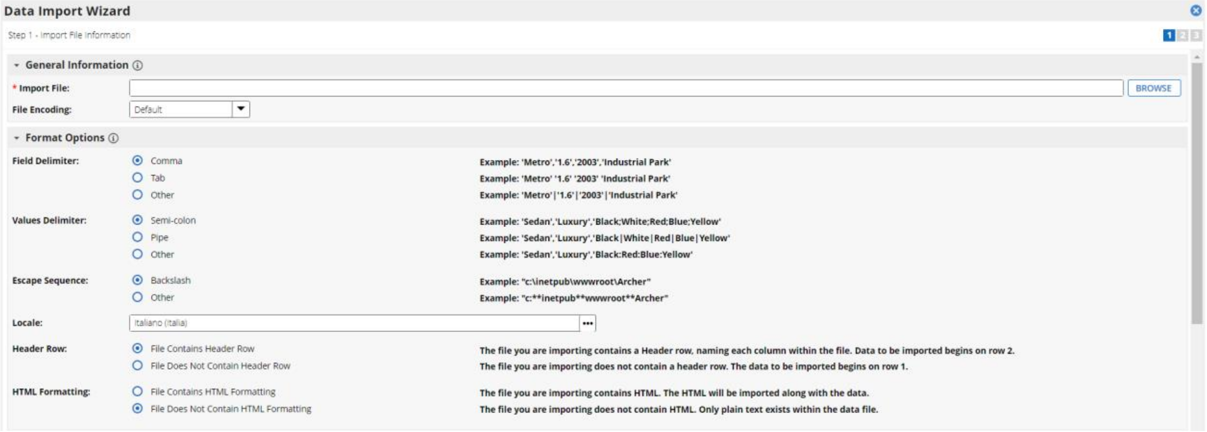
The fixed data still needed to be adapted to the right template for import. In particular, information from Archer needed to be added to the records to provide Archer with the references to insert the data where they belonged.

We took the company files in excel format and merged them with the information from Archer, through the INDEX-MATCH function. We adapted the column names to match with Archer field names and finally exported the excel files in csv format, tab delimited, to upload them in Archer.

7.3.1.3. Data import

The csv files were imported through the Archer interface shown in Figure 29.

The import wizard provides several options, and, in particular, the possibility to choose between creating new records and updating existing ones. In the second case, the user needs to select the lookup field to use as reference to match the values in the file to be uploaded with the records in Archer. In any case, the column names in the file must be mapped to the field names in Archer.



Data Import Wizard

Step 1 - Import File Information

▾ General Information ⓘ

* Import File: BROWSE

File Encoding: Default ▾

▾ Format Options ⓘ

Field Delimiter:
- ● Comma — Example: 'Metro','1.6','2003','Industrial Park'
- ○ Tab — Example: 'Metro' '1.6' '2003' 'Industrial Park'
- ○ Other — Example: 'Metro'|'1.6'|'2003'|'Industrial Park'

Values Delimiter:
- ● Semi-colon — Example: 'Sedan','Luxury','Black;White;Red;Blue;Yellow'
- ○ Pipe — Example: 'Sedan','Luxury','Black|White|Red|Blue|Yellow'
- ○ Other — Example: 'Sedan','Luxury','Black:Red:Blue:Yellow'

Escape Sequence:
- ● Backslash — Example: "c:\inetpub\wwwroot\Archer"
- ○ Other — Example: "c:\inetpubwwwroot**Archer"

Locale: Italiano (Italia) •••

Header Row:
- ● File Contains Header Row — The file you are importing contains a Header row, naming each column within the file. Data to be imported begins on row 2.
- ○ File Does Not Contain Header Row — The file you are importing does not contain a header row. The data to be imported begins on row 1.

HTML Formatting:
- ○ File Contains HTML Formatting — The file you are importing contains HTML. The HTML will be imported along with the data.
- ● File Does Not Contain HTML Formatting — The file you are importing does not contain HTML. Only plain text exists within the data file.

Figure 29: Import wizard

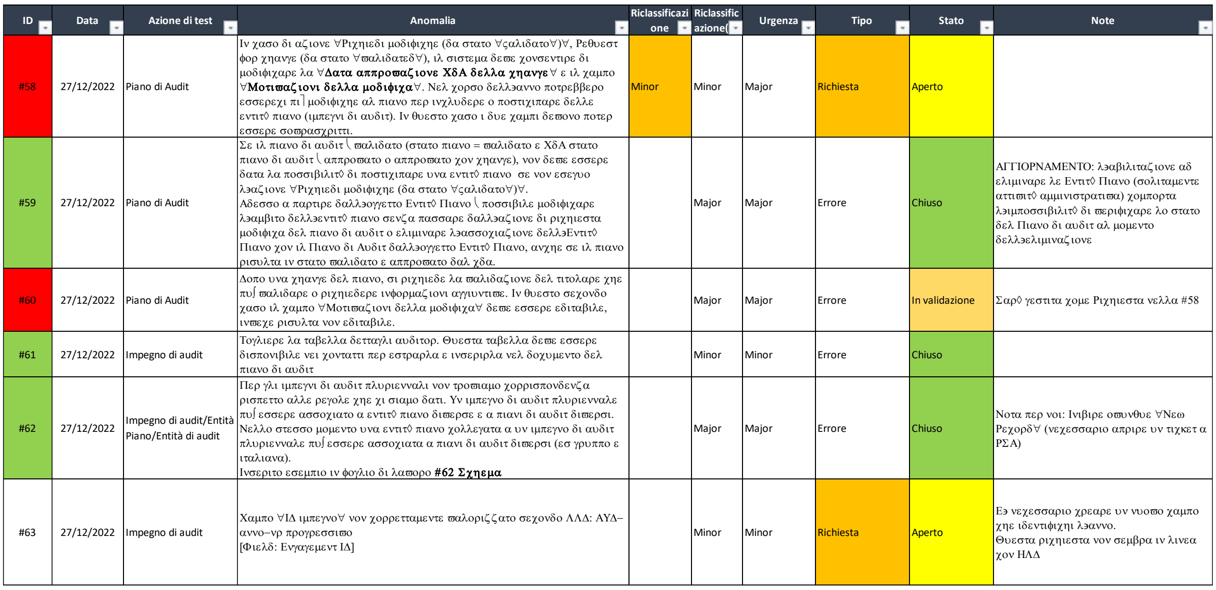
7.3.2. Bug fixing and change request management

The management of test results and correction/change requests was handled formally, through tracking lists (Figure 30), but without the use of ticketing software.

Bugs were immediately addressed by the consulting team, while change requests were evaluated by the project managers before starting system evolution activities.

7.4. Roll out

The roll-out can be divided into two sub-phases:



ID	Data	Azione di test	Anomalia	Riclassificazione	Riclassificazione(	Urgenza	Tipo	Stato	Note
#58	27/12/2022	Piano di Audit	Ιν χασο δι αζιονε ∀Ριχηιεδι μοδιφιχηε (δα στατο ∀ςαλιδατο∀)∀, Ρεθυεστ φορ χηανγε (δα στατο ∀ϖαλιδατεδ∀), ιλ σιστεμα δεϖε χονσεντιρε δι μοδιφιχαρε λα ∀**Δατα αππροϖαζιονε ΧδΑ δελλα χηανγε**∀ ε ιλ χαμπο ∀**Μοτιϖαζιονι δελλα μοδιφιχα**∀. Νελ χορσο δελλ∋αννο ποτρεββερο εσσερεχι πι⎤ μοδιφιχηε αλ πιανο περ ινχλυδερε ο ποστιχιπαρε δελλε εντιτ◊ πιανο (ιμπεγνι δι αυδιτ). Ιν θυεστο χασο ι δυε χαμπι δεϖονο ποτερ εσσερε σοϖρασχριττι.	Minor	Minor	Major	Richiesta	Aperto	
#59	27/12/2022	Piano di Audit	Σε ιλ πιανο δι αυδιτ ⎝ ϖαλιδατο (στατο πιανο = ϖαλιδατο ε ΧδΑ στατο πιανο δι αυδιτ ⎝ αππροϖατο ο αππροϖατο χον χηανγε), νον δεϖε εσσερε δατα λα ποσσιβιλιτ◊ δι ποστιχιπαρε υνα εντιτ◊ πιανο σε νον εσεγυο λ∋αζιονε ∀Ριχηιεδι μοδιφιχηε (δα στατο ∀ςαλιδατο∀)∀. Αδεσσο α παρτιρε δαλλ∋ογγεττο Εντιτ◊ Πιανο ⎝ ποσσιβιλε μοδιφιχαρε λ∋αμβιτο δελλ∋εντιτ◊ πιανο σενζα πασσαρε δαλλ∋αζιονε δι ριχηιεστα μοδιφιχα δελ πιανο δι αυδιτ ο ελιμιναρε λ∋ασσοχιαζιονε δελλ∋Εντιτ◊ Πιανο χον ιλ Πιανο δι Αυδιτ δαλλ∋ογγεττο Εντιτ◊ Πιανο, ανχηε σε ιλ πιανο ρισυλτα ιν στατο ϖαλιδατο ε αππροϖατο δαλ χδα.		Major	Major	Errore	Chiuso	ΑΓΓΙΟΡΝΑΜΕΝΤΟ: λ∋αβιλιταζιονε αδ ελιμιναρε λε Εντιτ◊ Πιανο (σολιταμεντε αττιϖιτ◊ αμμινιστρατιϖα) χομπορτα λ∋ιμποσσιβιλιτ◊ δι ϖεριφιχαρε λο στατο δελ Πιανο δι αυδιτ αλ μομεντο δελλ∋ελιμιναζιονε
#60	27/12/2022	Piano di Audit	Δοπο υνα χηανγε δελ πιανο, σι ριχηιεδε λα ϖαλιδαζιονε δελ τιτολαρε χηε πυ∫ ϖαλιδαρε ο ριχηιεδερε ινφορμαζιονι αγγιυντιϖε. Ιν θυεστο σεχονδο χασο ιλ χαμπο ∀Μοτιϖαζιονι δελλα μοδιφιχα∀ δεϖε εσσερε εδιταβιλε, ινϖεχε ρισυλτα νον εδιταβιλε.		Major	Major	Errore	In validazione	Σαρ◊ γεστιτα χομε Ριχηιεστα νελλα #58
#61	27/12/2022	Impegno di audit	Τογλιερε λα ταβελλα δετταγλι αυδιτορ. Θυεστα ταβελλα δεϖε εσσερε δισπονιβιλε νει χονταττι περ εστραρλα ε ινσεριρλα νελ δοχυμεντο δελ πιανο δι αυδιτ		Minor	Minor	Errore	Chiuso	
#62	27/12/2022	Impegno di audit/Entità Piano/Entità di audit	Περ γλι ιμπεγνι δι αυδιτ πλυριενναλι νον τροϖιαμο χορρισπονδενζα ρισπεττο αλλε ρεγολε χηε χι σιαμο δατι. Υν ιμπεγνο δι αυδιτ πλυριενναλε πυ∫ εσσερε ασσοχιατο α εντιτ◊ πιανο διϖερσε ε α πιανι δι αυδιτ διϖερσι. Νελλο στεσσο μομεντο υνα εντιτ◊ πιανο χολλεγατα α υν ιμπεγνο δι αυδιτ πλυριενναλε πυ∫ εσσερε ασσοχιατα α πιανι δι αυδιτ διϖερσι (εσ γρυππο ε ιταλιανα). Ινσεριτο εσεμπιο ιν φογλιο δι λαϖορο **#62 Σχημα**		Major	Major	Errore	Chiuso	Νοτα περ νοι: Ινιβιρε οϖυνθυε ∀Νεω Ρεχορδ∀ (νεχεσσαριο απριρε υν τιχκετ α ΡΣΑ)
#63	27/12/2022	Impegno di audit	Χαμπο ∀ΙΔ ιμπεγνο∀ νον χορρετταμεντε ϖαλοριζζατο σεχονδο ΛΛΔ: ΑΥΔ−αννο−νρ προγρεσσιϖο [Φιελδ: Ενγαγεμεντ ΙΔ]		Minor	Minor	Richiesta	Aperto	Ε∋ νεχεσσαριο χρεαρε υν νυοϖο χαμπο χηε ιδεντιφιχηι λ∋αννο. Θυεστα ριχηιεστα νον σεμβρα ιν λινεα χον ΗΛΔ

Figure 30: Example of tracking list (anonymized)

- Activation of Italian companies in the Italian language
- Cascade activation of the foreign companies of the group.

The roll-out began with the approval of UAT environment test results and the resolution of any fixes and ends with the system actually operating and users being able to use it independently.

The first roll-out involved several activities:

- Alignment of the production environment
- Populating the production environment (as previously described in the paragraph about testing)
- Training of key users
- Verification of activities after deployment.

Regarding training, users are divided into Solution Admins and Key Users; the latter are responsible for the daily use of the platform, while the former are mainly responsible for verifying the progress of activities, each for their own solution of interest, and formulating change requests. The roll-out to foreign companies, still in progress, involves a phase of translation of the system, for which Archer provides appropriate tools, and may involve small integrations of the solution, especially due to the regulatory specificities of different countries.

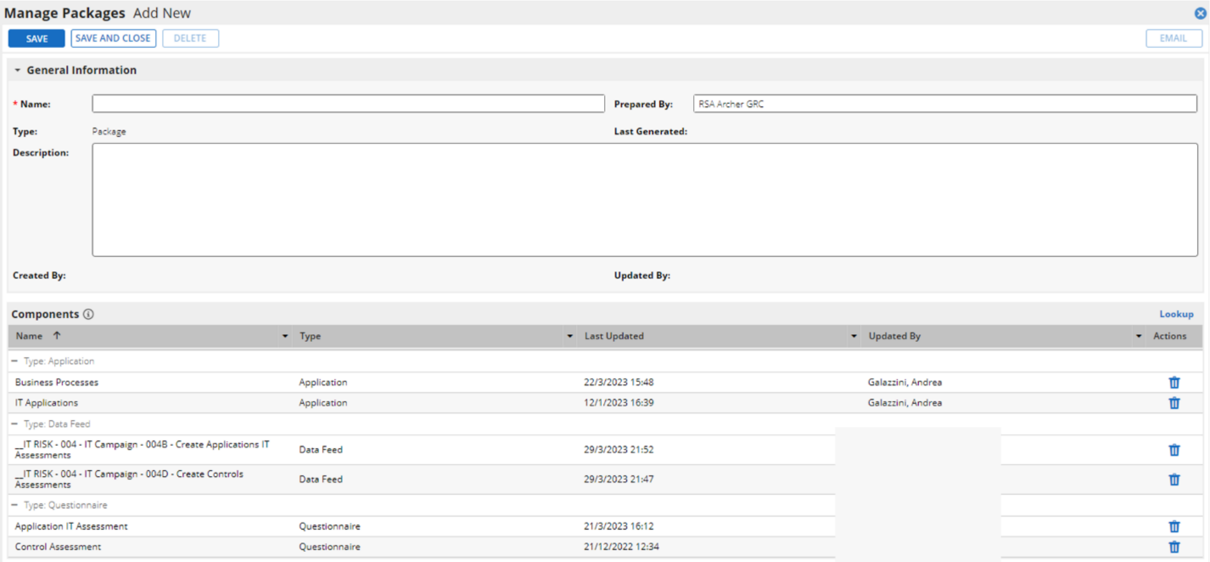
7.4.1. Alignment of the production environment

In Archer, the migration of the configuration from an environment to another consists of creating export packages in the source system and then import and map them in the destination environment. In this way we managed the migration from development to UAT system and from UAT to production system, avoiding the inefficiency and the risks of manually reproducing the changes of an environment into another.

A package can contain the different objects subject to customization such as:

- Applications
- Questionnaires
- Dashboards
- Access Roles
- Data Feeds.

The creation of a package (Figure 31) is very simple and simply asks to look up for the elements to be added to the package.



* Name:		Prepared By:	RSA Archer GRC
Type:	Package	Last Generated:	
Description:			
Created By:		Updated By:	

Components ⓘ Lookup

Name ↑	Type	Last Updated	Updated By	Actions
− Type: Application				
Business Processes	Application	22/3/2023 15:48	Galazzini, Andrea	🗑
IT Applications	Application	12/1/2023 16:39	Galazzini, Andrea	🗑
− Type: Data Feed				
__IT RISK - 004 - IT Campaign - 004B - Create Applications IT Assessments	Data Feed	29/3/2023 21:52		🗑
__IT RISK - 004 - IT Campaign - 004D - Create Controls Assessments	Data Feed	29/3/2023 21:47		🗑
− Type: Questionnaire				
Application IT Assessment	Questionnaire	21/3/2023 16:12		🗑
Control Assessment	Questionnaire	21/12/2022 12:34		🗑

Figure 31: Package creation

Once the package is created in an environment, the user needs to click generate to export it.

Once exported, the package is ready to be uploaded in another environment. To do so, after importing it into another environment, the user needs to specify whether the elements in the package are new, in substitution of existing ones or if existing elements are to be deleted.

After the import procedure, a log reports the results, including information on warnings and errors.

7.4.2. Population of the production environment

For what concerns the ETL process, with the due differences, it stands what is described in the paragraph about testing. What, instead, was specific of the roll out phase was the managing of users' profiles.

Following the requirements defined during the building stage, 120 access roles were created, divided among the different solution areas. 43 groups of users were defined to assign the roles collectively.

The company configured the LDAP system to assign the correct roles to users when they access the GRC. We managed the users' configuration to provide them with the correct language and international options.

In full operation, the system automatically assigns users to the respective processes, such as a process owner to its own process flows. While the automation wasn't already operational, we manually linked process owners to their processes through an import, while launching the production environment.

7.4.3. Training of the key users

The last step of the project, before the next phase (the maintenance), was the training of the key users of the system.

The agreement between the parties was that the consulting team would have prepared the training documentation in the form of slides with a double purpose: serve as a guide to be left to users to consult on their own and as teaching material to be shown during workshops.

The workshops were structured as four hours frontal lessons held by the consulting team remotely via Microsoft Teams. Each lesson repeated the same concepts to a different set of users, since they were too many to include them all in a single session.

The slides, as well as the lessons, had to precisely describe the operations that the end users must follow to complete their tasks. The process flow described in the workshops follows the workflow implemented in the GRC's applications, pointing out the role of each user in the chain and the interactions between each user action.

I, in particular, was charged of preparing and teaching the loss data collection flow (see Figure 32), which involved the following actors:

- Loss event creator: played by a process owner, creates the event itself and assigns it to a manager
- Loss event manager: played by the loss event creator or another process owner. It adds the loss elements to the event and validates the event or requests the validation to the responsible of the event.
- Process owner responsible of the event: depending on the value chain of the event, the role is played by a process owner and can add additional loss elements to the event. The responsible of the event can be asked by the manager to validate the event.
- Central/Local operational risk team: is the only one that can validate the cancellation of an event. Additionally, when the sum of losses produced by the loss elements exceeds a certain threshold, Central/Local must agree to the validation of the event, before it can pass in the "completed" status.

I started the preparation of the slides by reviewing the LDC process flow (Figure 32) in order to be sure to know exactly what goes on; then, I collected all the useful screenshots to illustrate each passage of the procedure, keeping in mind which specific role did what. Finally, I put together all the screenshot in a pack of slides, enriching the images with explanatory text of the various steps and highlighting the buttons and choices to be made.

We, then, reviewed together, as the consulting team, the material regarding the different solution areas so that each of us would have been able to present each area during the workshops.

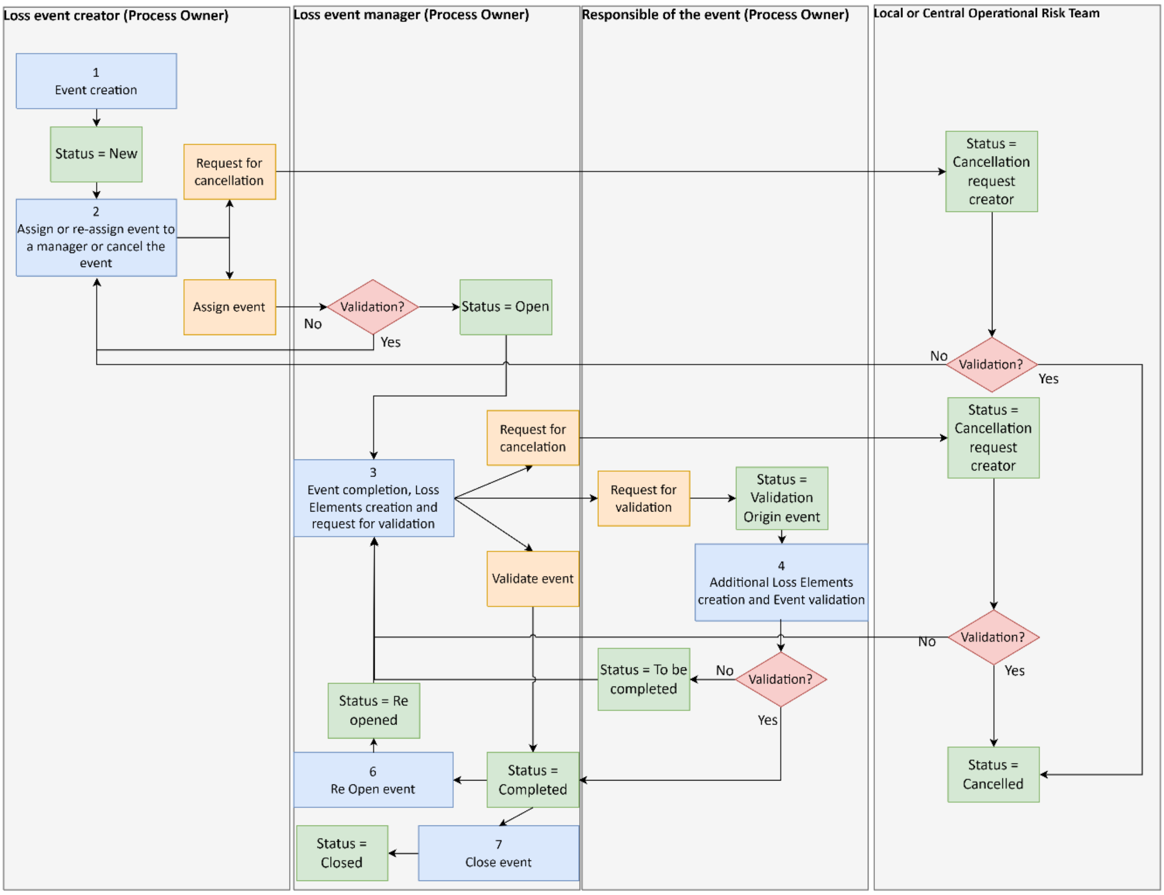

Loss event creator (Process Owner)
Loss event manager (Process Owner)
Responsible of the event (Process Owner)
Local or Central Operational Risk Team
1
Event creation
Status = New
Request for cancellation
2
Assign or re-assign event to a manager or cancel the event
Assign event
Validation?
No
Yes
Status = Open
Status = Cancellation request creator
No
Validation?
Yes
Request for cancellation
Status = Cancellation request creator
3
Event completion, Loss Elements creation and request for validation
Request for validation
Status = Validation Origin event
Validate event
4
Additional Loss Elements creation and Event validation
No
Validation?
Yes
Status = To be completed
No
Validation?
Yes
Status = Re opened
6
Re Open event
Status = Completed
Status = Cancelled
Status = Closed
7
Close event

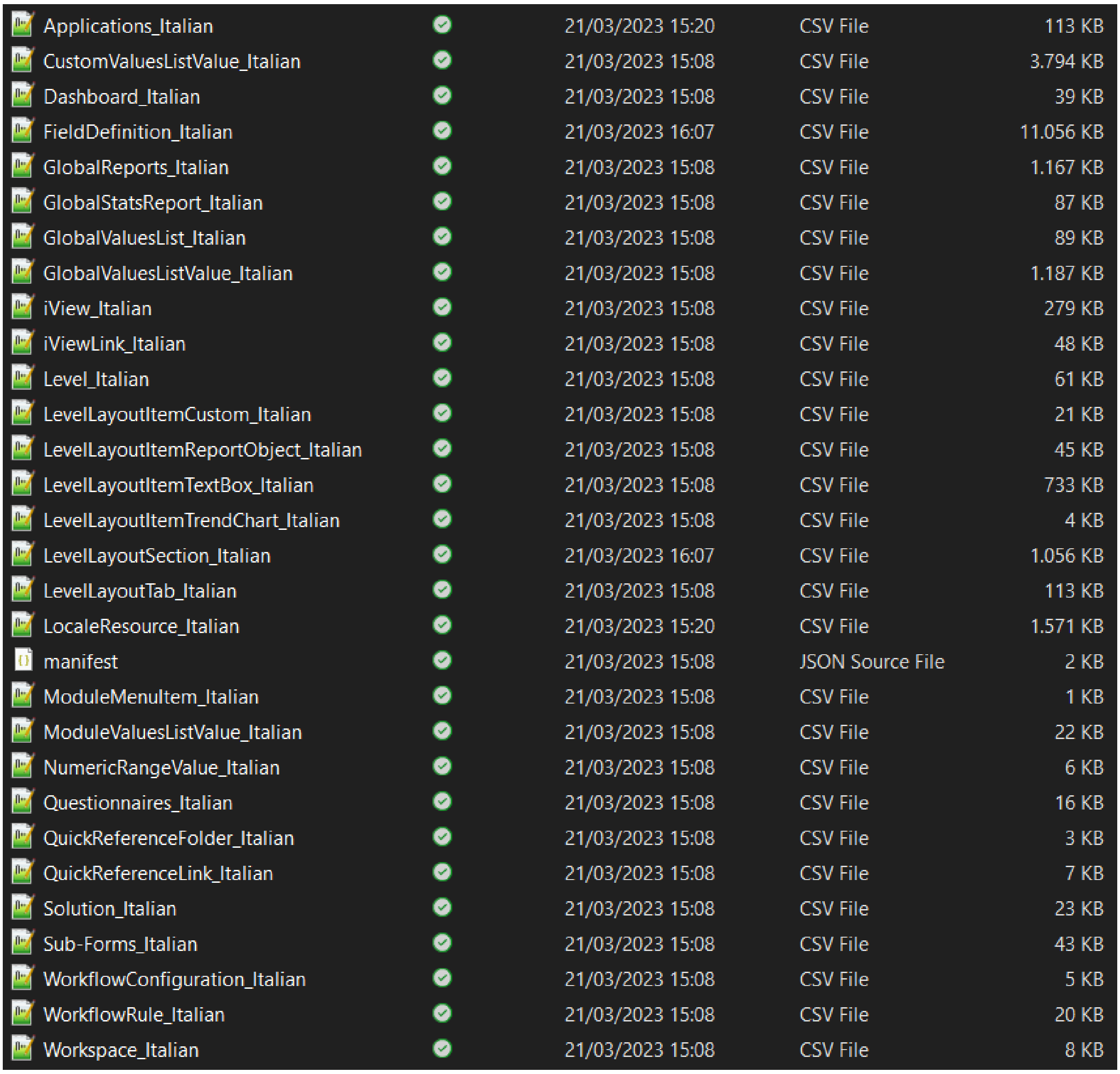
Figure 32: Loss data collection process flow

Ultimately, we split the workshops sessions between the team members and presented them to the company users.

7.4.4. Translations

Archer is provided in English, but the standard configuration already contains translations in various languages for the preinstalled features. For all the custom implementation we needed to translate applications, fields and everything else first in Italian and then in the foreign companies' languages.

Archer language configuration is not the smartest feature of the platform. In fact, Archer provides translation files (Figure 33), organized by Archer feature, which are not easy to navigate through.



Applications_Italian	✓	21/03/2023 15:20	CSV File	113 KB
CustomValuesListValue_Italian	✓	21/03/2023 15:08	CSV File	3.794 KB
Dashboard_Italian	✓	21/03/2023 15:08	CSV File	39 KB
FieldDefinition_Italian	✓	21/03/2023 16:07	CSV File	11.056 KB
GlobalReports_Italian	✓	21/03/2023 15:08	CSV File	1.167 KB
GlobalStatsReport_Italian	✓	21/03/2023 15:08	CSV File	87 KB
GlobalValuesList_Italian	✓	21/03/2023 15:08	CSV File	89 KB
GlobalValuesListValue_Italian	✓	21/03/2023 15:08	CSV File	1.187 KB
iView_Italian	✓	21/03/2023 15:08	CSV File	279 KB
iViewLink_Italian	✓	21/03/2023 15:08	CSV File	48 KB
Level_Italian	✓	21/03/2023 15:08	CSV File	61 KB
LevelLayoutItemCustom_Italian	✓	21/03/2023 15:08	CSV File	21 KB
LevelLayoutItemReportObject_Italian	✓	21/03/2023 15:08	CSV File	45 KB
LevelLayoutItemTextBox_Italian	✓	21/03/2023 15:08	CSV File	733 KB
LevelLayoutItemTrendChart_Italian	✓	21/03/2023 15:08	CSV File	4 KB
LevelLayoutSection_Italian	✓	21/03/2023 16:07	CSV File	1.056 KB
LevelLayoutTab_Italian	✓	21/03/2023 15:08	CSV File	113 KB
LocaleResource_Italian	✓	21/03/2023 15:20	CSV File	1.571 KB
manifest	✓	21/03/2023 15:08	JSON Source File	2 KB
ModuleMenuItem_Italian	✓	21/03/2023 15:08	CSV File	1 KB
ModuleValuesListValue_Italian	✓	21/03/2023 15:08	CSV File	22 KB
NumericRangeValue_Italian	✓	21/03/2023 15:08	CSV File	6 KB
Questionnaires_Italian	✓	21/03/2023 15:08	CSV File	16 KB
QuickReferenceFolder_Italian	✓	21/03/2023 15:08	CSV File	3 KB
QuickReferenceLink_Italian	✓	21/03/2023 15:08	CSV File	7 KB
Solution_Italian	✓	21/03/2023 15:08	CSV File	23 KB
Sub-Forms_Italian	✓	21/03/2023 15:08	CSV File	43 KB
WorkflowConfiguration_Italian	✓	21/03/2023 15:08	CSV File	5 KB
WorkflowRule_Italian	✓	21/03/2023 15:08	CSV File	20 KB
Workspace_Italian	✓	21/03/2023 15:08	CSV File	8 KB

Figure 33: Language configuration files

To add new translations, a user needs to download the translation files and then search them for the line with the item to translate and manually insert the translation, as in the following example:

"IT Applications >> Applications","Name","Effective Risk","Rischio netto","f6e44e8e-7020-4600-b74b-65507d7550c9","24055","1","9813f61f0a3e2438064e1bdb2d85a086".

Personally, we found that the easiest way to navigate the translation files was through the "Find in Files" feature of Notepad++, that allows users to look up for regular expressions throughout all the files present in a folder.

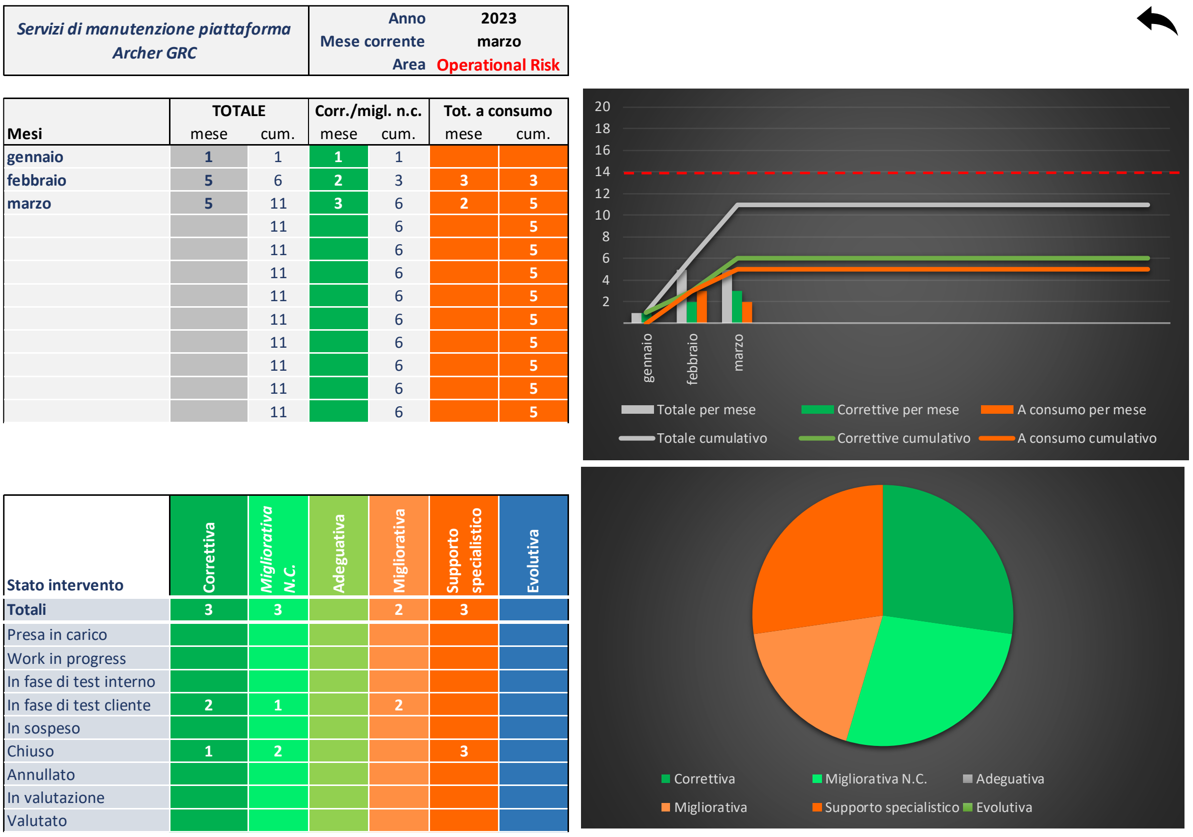
After that, to apply the translation, the user needs to import a zipped folder that contains the modified files along with a JSON manifest document.

7.5. Maintenance

The Application Maintenance activities began after the production roll-out and include:

- correction of errors that were not found in previous building and testing phases
- implementation of the changes, emerged during testing, that the project managers agreed on implementing
- requests for improvement changes that emerge as users become familiar with the new system
- application of patches to the platform.

Obviously, in this phase, bug fixing has priority in the workload, as continuity of service must be ensured as much as possible. Therefore, requests for improvement changes are queued to be evaluated by the project managers before being taken on. Requests for substantial modification or enrichment of the system's functionality and behavior are not part of the Application Maintenance activities; such evolutionary requests are subject to separate negotiation between the company and the consulting firm, as they require a commercial evaluation, a feasibility assessment, and a cost/benefit estimate.



Servizi di manutenzione piattaforma Archer GRC	Anno	2023
	Mese corrente	marzo
	Area	Operational Risk

	TOTALE		Corr./migl. n.c.		Tot. a consumo	
Mesi	mese	cum.	mese	cum.	mese	cum.
gennaio	1	1	1	1		
febbraio	5	6	2	3	3	3
marzo	5	11	3	6	2	5
		11		6		5
		11		6		5
		11		6		5
		11		6		5
		11		6		5
		11		6		5
		11		6		5
		11		6		5
		11		6		5

Stato intervento	Correttiva	*Migliorativa N.C.*	Adeguativa	Migliorativa	Supporto specialistico	Evolutiva
Totali	3	3		2	3	
Presa in carico						
Work in progress						
In fase di test interno						
In fase di test cliente	2	1		2		
In sospeso						
Chiuso	1	2			3	
Annullato						
In valutazione						
Valutato						

Figure 34: Application maintenance monitoring

Even in this phase, the management of test results and correction/change requests is handled formally, through tracking lists, but without using ticketing software. The way in which the tracking lists are managed allows for easy consultation of monitoring dashboards of activity progress, as shown in Figure 34.

However, it should be emphasized that, thanks to the rigorous testing procedures adopted in the project, the number of corrective actions requested to date is low and the severity is modest, allowing for a relatively quick average resolution time.

Regarding platform patches, the team regularly checks the release notes issued by the software supplier and evaluates the impact of their application.

In general, however, all patches are applied as soon as possible, in order to remain as aligned as possible with the latest version proposed by the supplier and to avoid congestion in the patching activity.

Although the supplier guarantees the quality of the patches, the work team undergoes a testing process before applying them, which is carried out first on development systems and then on UAT systems to avoid regression errors. Only if the UAT tests have a positive outcome can the patches be applied to production systems.

Any problems arising from the application of a patch are reported to the software supplier through its ticketing system.

8 Conclusion

The project was carried out within the expected timeframe and is providing satisfactory results.

The project stream I was mostly involved in (IT Risk Management) has been released in production for most of the functionalities originally defined in the building documents.

Additional functionalities, such as the management of remediation plans, are still under development and will be released as they pass UAT.

Further developments are also underway, such as the automation of data migration from Aris to Archer to keep the process map constantly aligned, the implementation of a sanction solution for the enterprise risk and others are under evaluation.

In my opinion, the main success factors of the project are:

- The commitment of the customer company management
- The effective collaboration between the parties involved
- The effectiveness of the project management methodology
- The quality of the dedicated resources in both the customer and the consulting team
- The soundness and flexibility of the adopted software
- The care in drawing up and following the design
- The effort in training the users and providing clear and exhaustive documentation.

In conclusion, taking part in this project has been a very positive experience to me. It was my first time being involved in a project that took place in the world of work, but nonetheless I managed to quickly integrate, thanks to the help and support of my colleagues. To me, the most interesting aspect has been the possibility to witness the whole life cycle of a project, assembling in a whole the various components that I learned as single parts during my academic studies.

Bibliography

[1] "Governance, Risk and Compliance (GRC)," [Online]. Available: https://www.gartner.com/en/information-technology/glossary/governance-risk-compliance-grc.

[2] «HSPI - CHI SIAMO,» [Online]. Available: https://www.hspi.it/chi-siamo/.

[3] "TXT Group - who we are," [Online]. Available: https://www.txtgroup.com/.

[4] «Report sulle minacce nel settore assicurativo e dei servizi finanziari,» [Online]. Available: https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-it-tr-financial-services-and-insurance.pdf.

[5] "2022 Data Breach Investigations Report," [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/.

[6] "VBA Stomp," [Online]. Available: https://vbastomp.com/.

[7] «Emotet: come proteggersi al meglio dal trojan,» [Online]. Available: https://www.kaspersky.it/resource-center/threats/emotet.

[8] "Introducing the Office 365 Attack Toolkit," [Online]. Available: https://www.mdsec.co.uk/2019/07/introducing-the-office-365-attack-toolkit/.

[9] "Pawn Storm Abuses OAuth In Social Engineering Attacks," [Online]. Available: https://www.trendmicro.com/en_us/research/17/d/pawn-storm-abuses-open-authentication-advanced-social-engineering-attacks.html.

[10] «IL RANSOMWARE AS A SERVICE (RAAS),» [Online]. Available: https://www.telsy.com/it/il-ransomware-as-a-service-raas/.

[11] "Aris," [Online]. Available: https://www.softwareag.com/en_corporate/platform/aris/.

[12] "Archer - about us," [Online]. Available: https://www.archerirm.com/about-us.

[13] Archer, "Archer Administration II - Student Guide".

[14] "Archer Integrated Risk Management," [Online]. Available: https://www.archerirm.com/_files/ugd/8a3f1d_245e921715d04d0bbdce9895e55a6741.pdf.

List of acronyms

DNS	Domain Name System
ERM	Enterprise Risk Management
ESG	Environmental, Social and Governance
ETL	Extract Transform and Load
GDPR	General Data Protection Regulation
GRC	Governance Risk and Compliance
IRM	Integrated Risk Management
ISO	International Organization for Standardization
IT	Information Technology
ITRM	Information Technology Risk Management
JSON	JavaScript Object Notation
LDAP	Lightweight Directory Access Protocol
LDC	Loss Data Collection
LOB	International Organization for Standardization
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
PMI	Project Management Institute
PMO	Project Management Office
RaaS	Ransomware as a Service
RACI	Responsible, Accountable, Consulted, Informed
RAD	Rapid Application Development
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SIM	Società di Intermediazione Mobiliare
SoW	Statement of Work

SOX	Sarbanes-Oxley Act
UAT	User Acceptance Testing
VBA	Visual Basic for Applications

List of Figures

Acknowledgments

I thank my colleagues in HSPI for the support I received during my internship.

I thank my mother and father for the opportunity to study and graduate at POLIMI.

I want to remember my beloved granny who would have really loved to see me graduated.