Ministry of Higher Education and Scientific Research

DR. YAHIA FARES UNIVERSITY OF MEDEA

Faculty of Science Department of Mathematics and Computer Science



Graduation Project

Submitted for graduation in Computer science master

Specialty: Systems Engineering and Web Technology

Title :

Dashboard Implementation Related to Operational Risk Management

Prepared by:

• Mr MAHDJOUBI Wassim

• Mr OUITIS Imed

Directed by:

• Mr. BENAISSA Khireddine

2021-2022

Abstract:

Management of operational risk is heavily dependent on manual processes and majority of the companies use conventional tools for implementation.
Risk information is being collated as a simple one-dimensional register and risk assessment is done based on subjective unit scores. However, these firms are beginning to realize the need for effective and efficient risk management practices to improve overall delivery of the services products in the market and company's financial performance through an integrated risk management solution.

Here comes the ORM solution which covers all the key modules including incident management and loss analytics, RCSA, KI and action plans, that empowers the organizations to effectively manage their operational risk within an enterprise risk framework. It combines powerful components of ORM enabling organizations to analyze, manage and mitigate operational risk in a simple and efficient manner.
Keywords : ORM, Operational Risk, Risk Assessment, financial performance, Risk management ,RCSA.

Résumé:

La gestion du risque opérationnel dépend fortement des processus manuels et la majorité des entreprises utilisent des outils conventionnels pour la mise en œuvre.

Les informations sur les risques sont rassemblées sous la forme d'un simple registre unidimensionnel et d'une évaluation des risques se fait sur la base de scores unitaires subjectifs. Cependant, ces entreprises commencent à se rendre compte la nécessité de pratiques de gestion des risques efficaces et efficientes pour améliorer la prestation globale des produits de services sur le marché et la société performance financière grâce à une solution intégrée de gestion des risques.

Voici la solution ORM qui couvre tous les modules clés, y compris la gestion des incidents et analyse des pertes, RCSA, KI et plans d'action, qui permettent aux organisations de gérer efficacement leurs risques opérationnels dans un cadre de risque d'entreprise. Elle associe de puissants composants de l'ORM permettant aux organisations d'analyser, de gérer et d'atténuer le risque opérationnel de manière simple et efficace.

Mots Clé : ORM, risque opérationnel, évaluation des risques, performance financière, gestion des risques, RCSA.

ملخص:

تعتمد إدارة المخاطر التشغيلية بشكل كبير على العمليات اليدوية وتستخدم غالبية الشركات الأدوات التقليدية للتنفيذ. يتم تجميع معلومات المخاطر كسجل بسيط أحادي البعد وتقييم المخاطر يتم على أساس درجات الوحدة الذاتية. ومع ذلك، بدأت هذه الشركات في تحقيق ذلك الحاجة إلى ممارسات إدارة مخاطر فعالة وكفؤة تحسين التسليم الشامل لمنتجات الخدمات في السوق والشركات الأداء المالي من خلال حل متكامل لإدارة المخاطر.

وخطط KI و RCSA الذي يغطي جميع الوحدات الرئيسية بما في ذلك الأحداث وتحليلات الخسارة و هنا يأتي حل ORM العمل ، التي تمكن المؤسسات من إدارة المخاطر ضمن إطار مخاطر المؤسسة. تدلّ أحجار الكارثة على الأساطير.

الكلمات المفتاحية

، المخاطر ، تقييم المخاطر ، الأداء المالي ، إدارة المخاطرRCSA، ORM

Table of Contents:

1 Chapter 1: risk management in banking activity 3
1.1 Risk 3
1.2 Risk Management 5
1.3 Operational Risk 6
1.3.1 People risk 7
1.3.2 Process risk 7
1.3.3 System and technology 7
1.3.4 External risk 8
1.4 Examples of Operational Risk 9
1.5 Identification of Operational Risks 10
1.5.1 Definition 10
1.5.2 Top-Down Model Vs Bottoms Up Model to Operational Risk Assessment 10
1.5.3 Problems with Risk Identification 12
1.5.4 Operational Risk Exposure 13
1.5.5 Operational Vulnerability 14
1.6 Data Collection 15
1.6.1 Internal Loss Data to Mitigate Operational Risk 15
1.6.1.1 What is internal Loss 15
1.6.1.2 Collection Of Internal Loss Data 15
1.6.1.3 Shortcoming Of Internal Loss Data 16
1.6.2 External Loss Data to Mitigate Operational Risk 18
1.6.2.1 What is External Loss 18
1.6.2.2 Why is External Loss Data Important? 18
1.6.2.3 How is External Loss Data Collected? 19
1.6.2.4 Limitations of External Loss Data 19
1.7 Risk Control: (RCSA) 20
1.7.1 what Is Risk Control? 20
1.7.2 How Risk Control Works? 20
1.7.3 What Does Risk Control Include? 22
1.7.4 Example Of Risk Control 23
1.7.5 What is Risk Control and Self Assessment (RCSA)? 23
1.7.6 Steps Followed During Risk Control and Self Assessment (RCSA) 24
1.7.6.1 Stage 1: Documentation and Definition 24
1.7.6.2 Stage 2: Identification of Risks 24
1.7.6.3 Stage 3: Assessment of Controls 25

1.7.6.4 Stage 4: Reviews and Ratings 25
1.8 Key Risk Indicators 26
1.8.1 What are Key Risk Indicators? 26
1.8.2 Designing the Key Risk Indicators 27
1.8.3 Difference Between KRIs and KPIs 27
1.8.4 Key Control Indicators 28
1.8.5 Challenges of Key Risk Indicators 28
1.9 Action Plans 29
1.9.1 What is a Risk action plan? 29
1.9.2 What is the purpose of a Risk action plan? 29
1.9.3 What are the different types of Risk action plans? 29
1.9.3.1 Risk Avoidance Plans 29
1.9.3.2 Risk Reduction Plans 29
1.9.4 Where does a Risk action plan fit into the risk management process? 29
1.10 The Followed model 30
2 Chapter 2: technologies & system implementation 31
2.1 Introduction 31
2.2 Site Rendering 31
2.3 Server-Side Rendering (Backend) 31
2.4 Client-Side Rendering (frontend) 32
2.5 Technologies used for backend development 32
2.6 Technologies used for backend development 33
2.7 BACKEND With Java Spring Boot 33
2.7.1 What is Micro Service? 33
2.7.2 Advantages 34
2.7.3 What is Spring Boot? 34
2.7.4 Advantages 34
2.7.5 Goals 34
2.7.6 Why Spring Boot? 35
2.7.7 How does it work? 35
2.7.8 Spring Boot Starters 36
2.7.8.1 Examples 36
2.7.9 Auto Configuration 38
2.7.10 Spring Boot Application 38
2.7.11 Component Scan 39
2.8 What is an API? 40

2.8.1 Types of APIs 41
2.8.2 Design Patterns 42
2.8.3 Design Patterns used in Spring Framework 43
2.8.4 What Is Hibernate in Spring Boot 45
2.8.5 How does JPA/Hibernate Work? 45
2.8.6 Important Concepts in JPA 45
2.8.7 JPA vs Hibernate 46
2.9 JavaMail 47
2.9.1 Protocols used in JavaMail API 47
2.9.2 JavaMail Architecture 48
2.9.3 Java Mail API in Spring Boot 49
2.10 What is Redis Cache? 49
2.10.1 What is Redis used for? 50
2.11 Spring Boot Security with Oauth2-JWT 51
2.12 Frontend With Angular: 52
2.12.1 Angular Essentials and Architecture 52
2.12.2 Modules 53
2.12.3 Components 54
2.12.4 Templates, Directives and Data binding 54
2.12.5 Services and Dependency injection 55
2.12.6 Routing 55
3 Chapter 3: conception and system design 57
3.1 Introduction 57
3.2 risk assessment Formula 58
3.3 General use case diagram 63
3.4 Authentication sequence diagram 64
3.5 Risk identification and assessment database tables 65
3.6 Incident Form Organigram 66
3.7 Loss data Organigram 67
3.8 RCSA Organigram 68
3.9 Key indicators Organigram 69
3.10 Action plan Organigram 70
4 Chapter 4 : ORM system under oversight 71
4.1 General Application Features 71
4.1.1 Application Login 71
4.1.2 Cross-Module Access & Integration 72

4.1.3 Navigation Bar 73
4.1.4 Listing Grids 74
4.1.5 Search Filters 75
4.1.6 Audit Trail 76
4.1.7 Preference Setting 76
4.1.8 Screen Optimization 78
4.1.8.1 Single process design 78
4.1.9 Notification and My Bucket 79
4.2 Administration 80
4.2.1 Introduction 80
4.2.2 Basic Information 80
4.2.3 Access Administration Page 81
4.2.4 Access Category Page 82
4.2.5 Workflows and Statuses 86
4.3 Loss Data 87
4.3.1 Introduction 87
4.3.2 Incident Proposals 88
4.3.3 Adding Incident Proposals 88
4.3.4 Detailed Incidents 90
4.3.5 Adding Detailed Incidents 91
4.4 Risk & Control Self-Assessment 94
4.4.1 Introduction 94
4.4.2 Risk Register 95
4.4.3 Risk Assessment 97
4.4.4 Control Register 99
4.4.5 Add Control 100
4.4.6 Risk Appetite Matrices Creation 102
4.5 Heat Map 103
4.6 Key Indicators 104
4.6.1 Introduction 104
4.6.2 Data Points 105
4.6.2.1 Adding New Data Points 106
4.6.3 Input 108
4.6.3.1 Adding New Input 109
4.6.4 Key Indicators 110
4.6.4.1 Adding New Key Indicators 110

4.6.5 Dashboard 107
4.7 Action Plans 108
4.7.1 Introduction 108
4.7.2 Manage Action Plans 108
4.7.2.1 Adding New Action Plans 109
5 Conclusion 111
6 References 112

Figures Liste :

Chapter 1 :

Figure 1. 1 : Risk Impact 4
Figure 1. 2 : Operational Risk 8
Figure 1. 3 : Principles of an ORM policy 12
Figure 1. 4 : Events Lifecycle 17
Figure 1. 5 : RCSA path to the next step 22
Figure 1. 6 : Key Operational Risk Indicator 26

Chapter 2 :

Figure 2. 1 : Microservices vs Monolithic architecture 33
Figure 2. 2 : How Api Work 40
Figure 2. 3:API Types by release Policies 42
Figure 2. 4 : JPA Architecture 46
Figure 2. 5 : JavaMail Architecture 48
Figure 2. 6 : java mail support in spring framework 49
Figure 2. 7 : how Redis is used 50
Figure 2. 8 : Angular Essentials 56

Chapter 3 :

Figure 3. 1 : Activity diagram of the proposed risk assessment approach 58
Figure 3. 2 : Activity diagram for identifying hazard score 60
Figure 3. 3 : Use Case Diagram 63
Figure 3. 4 : authentication sequence diagram 64
Figure 3. 5 : Database Tables 65

Chapter 4 :

Figure 4. 1 : Application Login 71
Figure 4. 2 : Module Selection 72
Figure 4. 3 : Navigation Bar 73
Figure 4. 4 : Listing Grid Features 74
Figure 4. 5 : Search Filters 75
Figure 4. 6 : System Audit 76
Figure 4. 7 : Preferences Option 77
Figure 4. 8 : Preferences 77
Figure 4. 9 : Single Process Design 78

Figure 4. 10 : Notifications 79
Figure 4. 11 : My Bucket 80
Figure 4. 12 : Access Administration Page 81
Figure 4. 13 : Workflow Setup 86
Figure 4. 14 : Incident Proposals 88
Figure 4. 15 : New Incident Proposal 89
Figure 4. 16 : Detailed Incidents 90
Figure 4. 17 : New Detailed Incident 91
Figure 4. 18 : Risk Register 95
Figure 4. 19 : New Risk Addition 96
Figure 4. 20 : Risk Assessment 98
Figure 4. 21 : Control Register 99
Figure 4. 22 : New Control Addition 100
Figure 4. 23 : RAM Creation Access 102
Figure 4. 24 : Heat Maps 103
Figure 4. 25 : Data Points 105
Figure 4. 26 : Create New Data Points 106
Figure 4. 27 : Input Page 108
Figure 4. 28 : New Input 109
Figure 4. 29 : Key Indicators 110
Figure 4. 30 : New Key Indicators 111
Figure 4. 31 : Dashboards 107
Figure 4. 32 : Manage Action Plans 108
Figure 4. 33 : New Action Plan 109

List of Abbreviations

R.A : risk assessment

I.R : inherent risk

R.R : residual risk

A.P : action Plan

KI : key indicators

UR: user rights

UP: user profile

BH: business hierarchy

DP: data point

ORM : operational risk management

R.C : risk champion

HOD : head of department

JWT : json web token

API: application protocol interface

JPQL: java persistance query language

Introduction

Introduction:

In its general form and as what's known, risk is the possibility of something bad happening. Risk involves uncertainty about the effects/implications of an activity with respect to something that humans value (such as health, well-being, wealth, property or the environment), often focusing on negative, undesirable consequences. Moreover, and by focusing on financial sector and banks, Risk is defined as the chance that an outcome or investment's actual gains will differ from an expected outcome or return. Risk includes the possibility of losing some or all of an original investment. Quantifiably, risk is usually assessed by considering historical behaviors and outcomes. In finance, standard deviation is a common metric associated with risk. Standard deviation provides a measure of the volatility of asset prices in comparison to their historical averages in a given time frame. Diving deeper, The Basel II committee (an international business standard that requires financial institutions to maintain enough cash reserves to cover risks incurred by operations) defines operational risk, which will be the main theme of this thesis, as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. This includes legal risk but excludes strategic and reputation risks, though a significant operational loss can affect the reputation.

Problematic:

The Basel II Accord provides three methods for calculating operational risk capital charges:

- the basic indicator modeles.
- the standardized model.
- the advanced measurement model (AMM).

The model for operational risk management for a bank depend on various factors, like the size and sophistication of the bank and the nature and complexity of its business. However, clear strategies and oversight by the board of directors and senior management, a strong operational risk and internal control culture, effective internal reporting and contingency planning are crucial elements of an effective operational risk management framework for banks of any size. Recently, AMM was the most elected model implemented by banks to satisfy their needs. For moving to the AMM, banks must track internal loss data and use it as the foundation of empirical risk estimates, as a means of validating the inputs and outputs of the risk management system. Internal loss data is most relevant when it is clearly linked to a bank's current business activities, technological processes and risk management procedures. Banks must also use scenario analysis of expert opinion in conjunction with external data to evaluate its exposure to high-severity events. This movement required an implementation of a resilient system that covers all these aspects and to facilitate the process for industries to track their internal and external data , creating the dashboard which is what we'll be doing in this thesis to cover these aspects .

Chapter 1
risk management in banking activity

1 Chapter 1: risk management in banking activity

1.1 Risk

The concept of risk is multifaceted and not always straightforward as can be seen from following studies. Referring to the ancient Greek and Italian, it becomes apparent that the word risk was used in uncertain situations and it meant “to dare” (Hamberg, 2000 & Picket, 2013, p.60). Therefore, as risk is unavoidable, humans and businesses need to dare among dynamic risk situations with unexpected outcomes (Kaplan & Garrick, 2006). It should be noted here that from early researches risk and uncertainty are not the same. According to Hamberg (2000) risk refers to situations where the probability of outcomes can be established while in uncertain situations the outcomes are unknown. Further, risk involves uncertainty,but it also might include some loss or damage (Kaplan & Garrick, 2006). In addition, what is considered risk, internal or external, in a given time might not be seen as such in future (Cornia, Dressel & Pfeil, 2014).

For a proper decision-making and to earn legitimate return on investments risks need to be weighed and measured (Kaplan & Garrick, 2006). Knowledge about the environment (Ganegoda & Evans, 2014) and the awareness of the outcomes then reduce the level of risk (Kaplan & Garrick, 2006). In business, “risks are assessed by the potential likelihood and financial impact they have, representing series of challenges that should be met and assessed” (COSO-framework cited in Picket, 2013, p.62). Assessing risks by identifying their likelihoodand financial impact then helps with classifying the major risks and spare resources on the most critical ones for the business. Figure 1.1 gives a more clear vision through this idea. The risks that are identified as high likelihood and high impact are marked as red which are the ones that threaten business more than other ones.

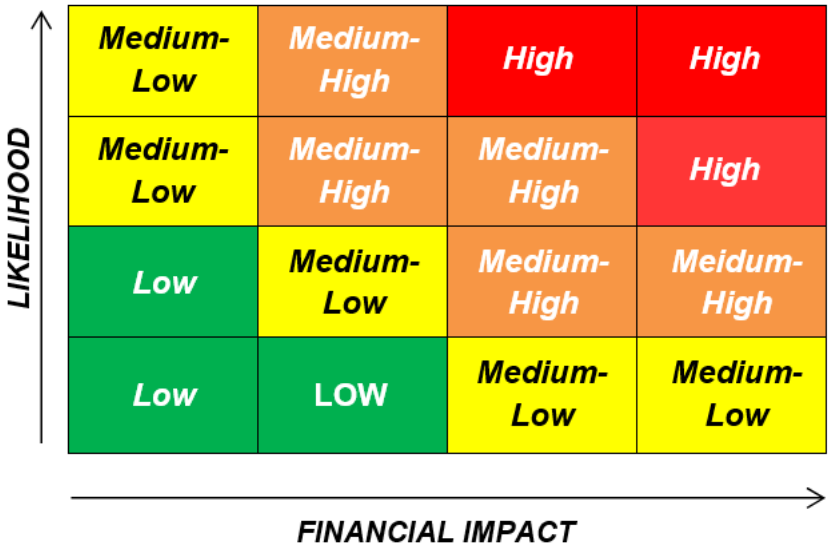


Figure 1. 1 : Risk Impact

However, the implication of risk also depends on these two factors: 1. *Risk Culture*, 2. *Risk Appetite*.

Weaknesses in risk culture are named among main factors affecting the recent crisis (Financial Stability Board, 2014). Just like culture, risk culture is "reflected in the attitudes, behavioral, and managerial norms" within an organization which will direct the institution into the way they face and manage risk challenges (Atkinson, 2013). Moreover, risk culture has been recognized as the building block of corporate governance and ORM (Roeschmann, 2014). Yet, financial institutions (especially banks) are still facing challenges when it comesto defining a clear risk culture (EY, 2013).

Within the framework of risk culture, appropriate risk appetite is recognized and the governance makes sure that no risks are taken beyond what the culture and appetite can handle. For building a stronger risk culture throughout the organization it is important to have an effective risk appetite framework (EY, 2013). Simply defined "risk appetite is the amount of risk to which the organization is prepared to be exposed before it judges action to be necessary" cited in Picket, 2013, p.71). The Swedish Financial Supervisory Authority (SFSA)in its latest set of regulations published in 2014 defined risk appetite as the "level and orientation of the undertaking risks that are acceptable

for achieving the strategic goals of the undertaking" (FFFS 2014:1). In order to implement the right risk appetite and manage risks properly, banks and financial institutions need to link the procedure to the planning process (Finansinspektionen Regulatory Code a). It should be noticed here that risk appetite is also a dynamic factor and changes from time to time depending on the level of risks threatening the business.

Therefore, it becomes apparent that within the concept of risk, risk culture and risk appetiteare also integral parts of effective bank operation and establish the basis for successful risk management.**[1]**

1.2 Risk Management

Risk management is the main component of success in finance and investment sector today. The need for implementation of effective risk management together with corporate governance was highlighted in the GFC (Aebi, Sabato & Schmid, 2011). By adopting sophisticated risk management practices and creating the possibility of having an appropriate and sound risk management strategy; the business then will increase the likelihood of long- term survival (Kim & Vonortas, 2014). It should be noted here that the risk management process has to be fully understood by the board of directors and senior executives as well as lower-level employees.

Before, risk management has been perceived as an operational activity instead of continuous responsibility of the board (Ingley & Walt, 2008). Currently, along with board's responsibility, risk management strategies usually focus on three main factors: meeting or exceeding an organization's objectives, adhering to control-based objectives and complying with regulatory requirements (COSO, 2013). In addition, according to a study done by Moody(2010) to increase the effectiveness of risk management in the organization, the risk management process should be part of organizational processes and decision making while it should be dynamic and responsive to changes.

Within the organizational goals set by the board of directors and senior management, risk management ensures that the process of identifying, measuring, controlling/monitoring and reviewing is implemented throughout the whole risk management process (Bank of International Settlements, u.d.). In addition, the risks

and the management plan should be mitigated and reported to the board. Further, to ensure that the risk management process is implemented accurately there should bean in-house Chief Risk Officer (CRO). CRO safeguards that all risks are strategically assessedwithin the corporate risk policy, the business is responding properly to new risks and challenges, and provides advice on sensitive risk issues for suitable decision-making (Picket, 2013, p.76-77). Overall, the CRO's task is to make sure that an effective internal control system is being implemented to manage the risks effectively. However, barriers such as insufficient strength of the process, inadequate risk managers, inappropriate risk analysis and unsatisfactory attitude towards risk should be understood by the CRO when assessing the risk management plan (Carter & Chinyio, 2012). This is why it is worth to make ongoing improvement on the way banks manage the risk effectively.[2]

1.3 Operational Risk

Besides credit, liquidity and market, operational risk is the other significant risk in banks. These risks are all interconnected to each other, but for the purpose of this thesis the focus is only on operational risks and how they should be managed. Thus, in case of the absence of operating loss as the biggest loss, all other types of failures are considerably less important. Further, many banks have collapsed and experienced financial problem because of ineffective risk management system in general and ORM in particular, especially important this issue became after GFC. Although, the last financial crisis has been generally characterized as a liquidity crisis, operational risk and its factors played a significant role in crisis length and severity (Jongh & Vuuren, 2013). Therefore, the need to explore the concept of operational risk has increased significantly. During long period of time, operational risk remained a residual category for uncertainties which was difficult to identify and measure in traditional ways (Power, 2005). In the last decade, increasing interest to operational risk caused the release of standards and frameworks. The general definition of operational risk provided by such frameworks is "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events". This definition

includes legal risk, but excludes reputational risk (BCBS, 2006, p.144). SFSA addresses the diversity of institutions by providing alternative modeles for calculating operational risk capital requirements concerning different levels of risk-sensitivity and sophistication (Finansinspektionen Regulatory Code a). There are only few detailed studies done by scholars on operational risk and its factors. For the purpose of this thesis, the literature on operational risk aspects are to a major extent based on a study done by Jarrow in 2008. Authors believe this study provided the most detailed information on each factor, but some additional sources are used for a better understanding of some of the concepts. Below is the definition of each concept: 8 [3]

1.3.1 People risk

People risk includes the risk of loss associated with errors and illegal actions of Bank's employees, their lack of qualifications, improper organization of work in the bank, etc. People risk can also involve human error, insufficient training and management of personnel, lack of segregation of duties, lack of honesty and integrity.

1.3.2 Process risk

Process risk is the risk of loss associated with errors during operations and calculations, accounting, reporting, pricing, etc. The risk includes the implementation of transactions on all stages and other aspects of managing a business such as products and services risk, imperfect control system and lack of security or tough security.

1.3.3 System and technology

System and technology risk Implementation of IT into business environment brings challenges to workflow, procedures and policies, which in turn can lead to risks. Thus, risks associated with IT cannot be considered independently, but only in connection with people, process and other related risks (Fheili, 2011). IT system problems caused by viruses, cyber-attacks and other failures lead to significant problems which influence the whole organization. Therefore, system and technology risk can be classified as the risks of losses due to imperfect technology used in the banks, e.g. the lack of systems capacity, their inadequacy in relation to the ongoing operations, inappropriate data processing methods, poor quality or the inadequacy of data used. Using effective IT analysis and management together with providing IT

security will lead to successful functioning of the entire risk management system (Culbertson, 2004).

1.3.4 External risk

External risk is the risk of loss associated with changes in the environment in which the bank operates. Changes in legislation, politics, economics, and the risk of external physical interference in organization's activities are other major external risks.[3]

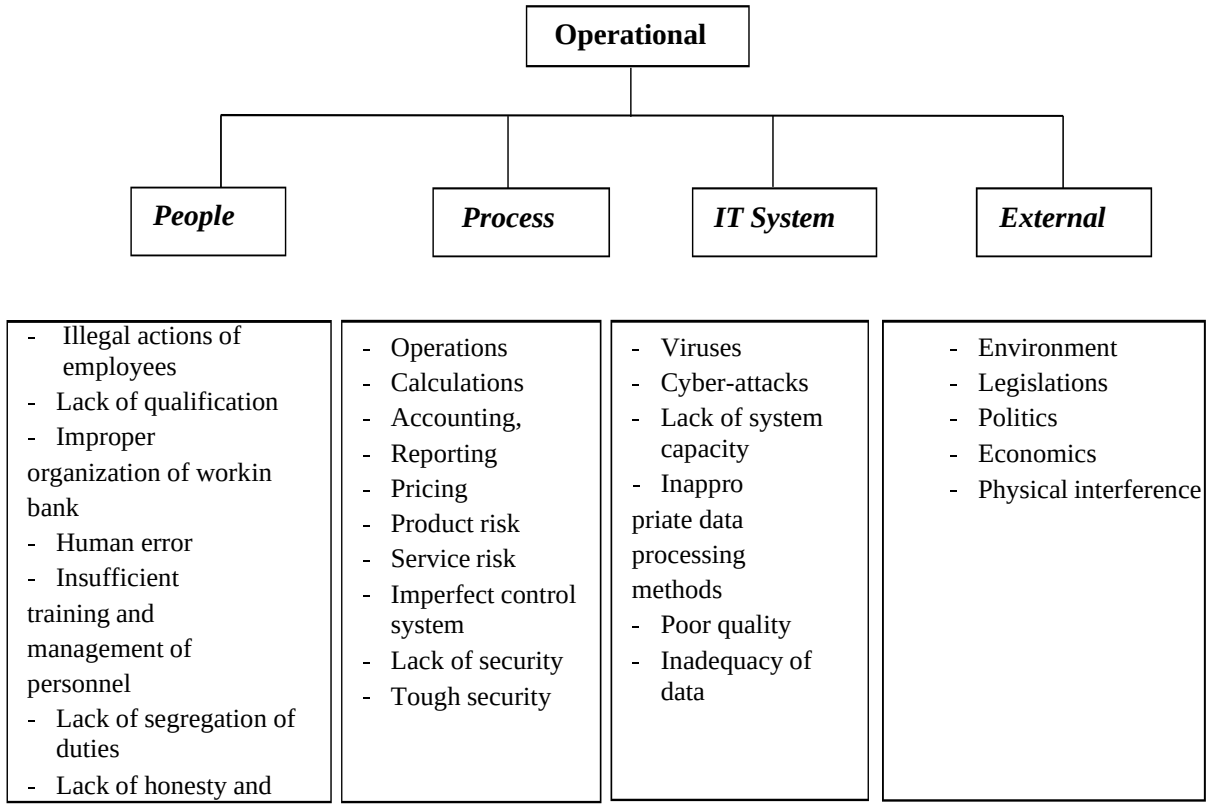


Figure 1. 2 : Operational Risk

1.4 Examples of Operational Risk

Many organizations have faced loss because of operational risks. Most of the time the losses are small. Hence, they are not reported in the media. As a result, awareness about these losses is not increased. However, in some cases, the losses are quite significant and hence end up being reported in the media. Some examples of these high profile adverse events related to operational risk are as follows:

There have been several financial frauds such as Enron, Worldcom, Bernie Maddoff scam, or the scam involving Raj Rajaratnam. These are all premier examples of how a group of incompetent or dishonest people is able to cause grievous loss to their organizations. Sometimes the loss is so severe that these organizations cease to exist as a result! The recent scam involving Facebook and Cambridge Analytica can also be included here because here too the actions of some contractors ended up harming the organization.

There are many examples wherein the systems of organizations have failed and as a result, the organization has suffered significant losses. For instance, many technology companies have been victims of cyber attacks in the recent past. Companies like Adobe, eBay, Equifax, and even LinkedIn have been found themselves at the center of many data leaks. This is also the case with many banks and financial institutions. Since data is vital to the performance of business activities in this organization, these data breaches have significantly impacted the business of these companies.

Lastly, there are many examples wherein processes set by organizations have failed. For instance, companies like Renault and Hyundai have been in the news. This is because some of their internal checks and balances failed. Their quality assurance team was not able to properly classify vehicles. As a result, faulty vehicles were sold. The end result was that these faulty vehicles had to be recalled and the organization had to suffer significant operational harm even if the reputational harm is not considered.

The bottom line is that there a clear and concise definition of operational risk which is in place. The drivers and causes of operational risk are also well known. It is this knowledge that enables the measurement and management of operational risks in the organization.

1.5 Identification of Operational Risks

1.5.1 Definition

The fundamental principle of operational risk management is to ensure that all operational risks have been considered and decisions have been taken about the best way to mitigate them. This is because experience has shown organizations that the worst outcomes come from risks that they have knowingly or unknowingly ignored. It is therefore important to ensure that the organization tries to maintain an exhaustive list of all the operational risks that it faces.

The reality is that the risk can never be exhaustive. However, the idea is to make the analysis as comprehensive as possible given the time constraints that the organization has. It is also important to realize that the identification of operational risks is not a one-time process. Since the organization operates in a dynamic environment, it is important to periodically scan the environment in order to identify newer risks that may emerge and proactively manage them.[4]

1.5.2 Top-Down Model Vs Bottoms Up Model to Operational Risk Assessment

The identification of operational risks is one of the most crucial steps in managing risks. The failure to identify risks almost certainly means that the organization will not take any action to mitigate them. Hence, to identify risks, a thorough scan of the entire organization and its operating environment is necessary. This is the reason that companies often use a combination of a top-down model as well as the bottom-up model in their bid to identify operational risks.

The top-down level of risk identification starts with the actions of the senior management. This is because the data required to conduct the top-down analysis is not available to people working at lower levels. Top-down risk identification is generally done by the senior management in seminars. The major process owners of the organization try to brainstorm about what could go wrong with their operations. These sessions include scenario generation exercises wherein the executives are supposed to

come up with the probable scenarios that the external environment can bring up and the response that the organization would give in each case. Generally, the top-down model considers emerging technology and global risks in their meetings. This type of risk analysis happens quite infrequently. This is because the external environment does not change very often.

As the name suggests, the bottom-up model to risk management is the opposite of the top-down model. This is because **the bottom-up model is often undertaken by supervisors and mid-level management**. However, they take their inputs from the lowest levels of workers. Process mapping and interviews are some of the most common techniques which are used in bottoms-up management. This is because the idea is to map the entire process at a granular level. Interviews help identify the most common threats to which the process is vulnerable. Also, it is the job of the management to conduct an operational risk analysis to identify key people and systems which can cause a systemic breakdown in the organization. This risk identification focuses on how technology and people can be deployed to provide optimum results for the company. However, there is an inherent issue with the bottoms up model. Many times, managers are too engrossed in finding their individual risks. Hence, the exercise is conducted on a very micro level. The end result of such an exercise is the identification of a series of disjointed risks. These risks may not have any pattern to them and maybe at a very low level. Hence, formulating an organization-wide model to mitigating these risks might become difficult in such an environment. The frequency of this process is quite high. Companies often conduct half-yearly or annual risk audits in order to identify the risks and create plans to mitigate them.[4]



Figure 1. 3 : Principles of an ORM policy

1.5.3 Problems with Risk Identification

The problem with risk identification is that it is not a process-based model. The methods used in the risk assessment exercise are qualitative. Hence, the outcomes of such methods are not consistent. For instance, two different groups at the same organization may brainstorm in order to identify risks and both the groups may come up with entirely different outputs. Both the bottoms up and top-down model relies on intuition and judgment instead of using the scientific method. Even after the risks are identified the categorization of these risks is subject to a lot of human judgment. This creates a huge problem since if the person conducting the risk management exercise is not competent, the risk identification would be incomplete. Tools like risk matrix have been created to help managers identify and prioritize risks. However, they too work based on the inputs given to them by the person identifying the risks.

The bottom line is that the identification of risks is an imperfect process. This is the reason that it needs to be done in an iterative manner. This is because it is possible that a risk that was missed the first time may be identified in the second or third attempt.[4]

1.5.4 Operational Risk Exposure

Risk exposure is defined as a measure of the possibility of future loss which may arise from a specific process or event. Exposure is related to the activities themselves whereas risk is the probability of an adverse event occurring while conducting those activities.

During the natural course of business, companies tend to engage in a lot of activities that increase their exposure to operational risks. Some of these activities have been mentioned below :

- Companies may route their products to the market via some key distribution channels. Hence, companies have large exposure to such channels. This could create operational risk in the future. For instance, the distributor might themself go out of business. Alternatively, the distributor may start distributing for another company which gives them a higher margin. Other times, geopolitical events and government rules may prevent the company from effectively using the services to be provided by the distributor.
- The company may rely on a handful of clients to generate the majority of its revenue. This creates exposure towards those clients. There is a possibility that those clients may go bankrupt or may find an alternate supplier. It is also possible that those clients may try to leverage their bargaining power and offer very low rates to the company thereby adversely impacting the profit margin.
- In many cases, companies are also dependent upon the services of some suppliers and key third parties. In such cases also, the company faces a similar set of challenges. The supplier may not be able to provide timely supply to our company. Also, the supplier may increase prices thereby disrupting the profit margin of the company
- Companies may also have exposure to some critical IT systems. The business may be largely driven by the flow of information which is enabled by these IT systems. If the suppliers to these systems stop providing support, the company may find it expensive and time-consuming to transition to a new product.
- Also, there is always the operational risk related to regulations. American companies trading with China have recently found out that their efficient and optimized business model can also be completely disrupted and uprooted for no fault of theirs. There is

always a risk that a new regulatory framework may be created which would adversely affect the business interests of the company

If you tried to map operational risk exposure on a risk matrix, it would be mapped in a high impact low probability zone. This means that the probability of any of these events mentioned above happening is very low. However, if it does happen then the impact will be significant. .[5]

1.5.5 Operational Vulnerability

Operational vulnerabilities on the other hand are low impact, high-frequency events. These events are much more likely to occur and even keep happening in the day-to-day life of any company. However, their financial impact is not that high. Operational vulnerabilities are often defined as the weakest link in any business process.

Defects or shortcomings in the day-to-day processes of the company are referred to as operational vulnerabilities. For instance, it is quite possible that a company may manufacture defective products or sometimes may ship the wrong product to the wrong customer. If these events occur, the company can quickly replace the product and provide the right order to the customer. They can even provide some freebies to ensure customer satisfaction. Hence, the cost will be low. However, these events happen quite often in some companies.

There is always a chance that the information system of a company crashes due to high data load. It is not unheard of for companies to stop functioning for a couple of hours or even a couple of days due to defects in their information systems. The financial impact of such outages is relatively low. However, they tend to happen more frequently

Incompetent personnel is also an operational risk to the business. There are some companies that routinely hire inexperienced people and then train them. In such cases, it is quite possible that the service level of the company may drop because of the inexperienced people providing the service. This is another important operational vulnerability that may cost the company in the long run. It is quite possible that each company may have some silos wherein a small group of people will continue to operate unabated without following the proper risk management protocols.

The goal of operational risk management is to thoroughly assess the exposures and vulnerabilities. Once they have been identified, the goal is to minimize the exposure. It is important to realize that exposures cannot be completely eliminated. However, at the same time, it is important to eliminate the vulnerabilities. Multinational companies spend a lot of their time and money ensuring that their processes are six sigma compliant and are therefore devoid of operational vulnerabilities.[5]

1.6 Data Collection

1.6.1 Internal Loss Data to Mitigate Operational Risk

1.6.1.1 What is internal Loss

Internal losses are losses that have arisen due to failed processes or incompetent people within the organization. The losses which occur may be financial or non-financial in nature. The objective of analyzing internal loss is:

- to categorize the operational losses by functions such as technology, human resources, marketing, etc
- to categorize operational risks by product categories, locations, and even by manager
- to identify and categorize risks that may come into play if the company decides to outsource some of its internal processes
- to create a priority list of all the internal risks so that appropriate risk mitigation mechanisms can be employed.[6]

1.6.1.2 Collection Of Internal Loss Data

Before data regarding internal loss is collected from the various parts of the organization, it is essential to generate buy-in from the different stakeholders. This is because organizations are by nature forward-looking. If the management asks for extensive data collection about past events, it is likely that they may face some resistance. Loss data collection is an exhaustive process. When implemented, it becomes part of the daily duty of every employee across the organization and a part of the daily business and usual functioning.

The objectives of loss data collection and the benefits that will be derived from it must be explained to all stakeholders in order to avoid issues later on.

- The first step is to create a procedure for identifying and booking internal losses. This means that a system has to be created using which losses can be identified, approved, and then booked i.e. recorded
- Subject matter experts have to be developed so that they are able to recognize internal losses and categorize them correctly before booking. The ideal process is that the front-line employee initiates the process by suggesting a loss that needs to be booked. This loss is then evaluated by an expert and then finally booked
- Separate accounts must be in place to book these expenses. These accounts can then be used to identify patterns in the internal losses or collect information about their drivers. Separate accounts also make it easy to identify the quantum of money that is being lost due to internal losses
- The process needs to have controls, checks, and balances in place. This means that there should be appropriate governance measures in place to prevent wrong data from being collected. The stakeholders of this process should continuously liaise with the compliance and audit partners in order to make sure that their process is functioning at the optimal level
- In recent years, the emphasis has been on the removal of manual processes and the implementation of automatic workflow-based processes. This makes it easier to capture data and ensure consistency across the process at different times. [6]

1.6.1.3 Shortcoming Of Internal Loss Data

There are several obvious benefits to internal loss data collection. However, there are several shortcomings as well. Some of them have been mentioned below:

1. Firstly, the internal loss collection process is too expensive and time-consuming. Basel norms specify that at least three years of data need to be collected in order to ensure that the organization is compliant with the norms. This leads to a lot of resources being deployed in order to meet these needs. These resources could have been used for other more productive purposes

2. Another problem with the model is that it always looks backward. It is a known fact that the future may not necessarily be like the past. However, the collection of internal loss data makes managers fixated with previous losses. This leads to improper risk management and mitigation.
3. Also, the internal loss collection framework has no mechanism for collecting data on potential losses or near misses i.e. losses that almost occurred. Hence, even if the organization may be susceptible to the same risks in the future, the data is not collected since an actual loss has not occurred! Hence, it can be said that the model is reactive and not proactive.
4. In some organizations, the definition of loss changes over a period of time. This creates a new set of challenges. This is because the data from previous years can no longer be compared to the present before modifying it to nullify the effect of the change in definition.

   The bottom line is that the collection of internal loss data is an integral part of the operational risk management process. The end result of this data collection is the creation of a loss database that can be used to better predict and mitigate future risks. This is the reason why this model is suggested in the Basel II norms and is likely to be implemented in major organizations all across the world. [6]



Figure 1. 4 : Events Lifecycle

1.6.2 External Loss Data to Mitigate Operational Risk

1.6.2.1 What is External Loss

External loss data is the data relating to losses that were suffered by other firms in the same industry or even in different industries as a result of operational risk. The key point to note here is that the loss happens because of operational risks. Also, it is important to note that since the data is generated outside the boundaries of the organization, the company has no way to capture the data directly.[7]

1.6.2.2 Why is External Loss Data Important?

External loss data helps a company in benchmarking its risk management standards to peer companies. It helps risk managers introspect and consider that if an event can happen in another company why wouldn't it happen in their company and what are the measures they are taking to protect themselves

External loss data is also useful in getting the necessary resources sanctioned from the senior management. Senior management is much more receptive to a pitch for resources if they see that a similar event has already happened at a peer firm. Hence, external loss data helps drive the culture of risk management in the firm's DNA

Over time, external loss data has become extremely reliable. This is because of the fact that the data is being collected for a period of more than thirty years. Hence, now it can be subject to statistical analysis and risk modeling. If data is collected over larger periods of time, it becomes more accurate since the effects of any specific variables that distort the results wear out over time. The reliability of external loss data makes money well spent for the organization

External loss data is widely used to develop scenarios for scenario analysis. This is because the data has been collected over a long period of time and hence the probability of various scenarios can be accurately collected. The profile of risk that the organization would be facing in different scenarios as well as the monetary loss that it would impose are points of contention.

External loss data helps to find the correlations between the operational risk faced by an individual firm with the risks being faced by an industry as a whole. This correlation helps them to understand the nature of the risks and investigate their root causes. For instance, some risks may be cyclical and may appear in every economic downturn regardless of the level of operational preparedness. [7]

1.6.2.3 How is External Loss Data Collected?

External loss data is data that originates in other companies. Hence, companies do not have any mechanism to access the data directly. They have to pay to access the data from other sources. This generally happens in one of the two ways.

Companies can buy access to a subscription loss database. Here the company has to pay cash in order to be able to access risk data related to other organizations. The name of the other organizations is generally kept anonymous. There is some sort of analysis that has already been conducted on the data. It is not uncommon for the data to be divided into different categories of risks, products, and lines of business. It is important to note that in this case cash is being exchanged for data

Companies can also decide to give access to their data in exchange for the data of other companies. There are consortiums in which companies can join and share their own data and at the same time get access to the data of other companies. It is important to note that here the company may not have to pay cash. Generally, a small amount has to be paid for the maintenance and upkeep of the consortium. However, it costs much less as compared to subscription databases. [7]

1.6.2.4 Limitations of External Loss Data

External loss data is helpful to a certain extent. However, it is important to note that the basic driving factors such as humans, processes, and systems are different in each company. Hence, even if firms operate within the same industry, they may face different risks. This is because of the quality of people or the systems that they may have deployed. Also, companies within the same industries operate with different types of vendors and clients. This makes their external risk profile somewhat unique. Hence,

external loss data should be considered as a beginning point of an analysis which may have to be refined further.The bottom line is that external loss data is considered mandatory since it has become a part of the Basel risk norms. However, many companies still find its usefulness to be limited. [7]

1.7 Risk Control: (RCSA)

1.7.1 what Is Risk Control?

Risk control is the set of methods by which firms evaluate potential losses and take action to reduce or eliminate such threats. It is a technique that utilizes findings from risk assessments, which involve identifying potential risk factors in a company's operations, such as technical and non-technical aspects of the business, financial policies and other issues that may affect the well-being of the firm.

Risk control also implements proactive changes to reduce risk in these areas. Risk control thus helps companies limit lost assets and income. Risk control is a key component of a company's enterprise risk management (ERM) protocol.[8]

1.7.2 How Risk Control Works?

Modern businesses face a diverse collection of obstacles, competitors, and potential dangers. Risk control is a plan-based business strategy that aims to identify, assess, and prepare for any dangers, hazards, and other potentials for disaster—both physical and figurative—that may interfere with an organization's operations and objectives. The core concepts of risk control include:

- Avoidance is the best method of loss control. For example, after discovering that a chemical used in manufacturing a company’s goods is dangerous for the workers, a factory owner finds a safe substitute chemical to protect the workers’ health.
- Loss prevention accepts a risk but attempts to minimize the loss rather than eliminate it. For example, inventory stored in a warehouse is susceptible to theft. Since there is no way to avoid it, a loss prevention program is put in place. The program includes patrolling security guards, video cameras and secured storage facilities. Insurance is another example of risk prevention that is outsourced to a third party by contract.

- Loss reduction accepts the risk and seeks to limit losses when a threat occurs. For example, a company storing flammable material in a warehouse installs state-of-the-art water sprinklers for minimizing damage in case of fire.
- Separation involves dispersing key assets so that catastrophic events at one location affect the business only at that location. If all assets were in the same place, the business would face more serious issues. For example, a company utilizes a geographically diverse workforce so that production may continue when issues arise at one warehouse.
- Duplication involves creating a backup plan, often by using technology. For example, because information system server failure would stop a company's operations, a backup server is readily available in case the primary server fails.
- Diversification allocates business resources for creating multiple lines of business offering a variety of products or services in different industries. A significant revenue loss from one line will not result in irreparable harm to the company's bottom line. For example, in addition to serving food, a restaurant has grocery stores carry its line of salad dressings, marinades, and sauces.

No one risk control technique will be a golden bullet to keep a company free from potential harm. In practice, these techniques are used in tandem with one another to varying degree and change as the corporation grows, as the economy changes, and as the competitive landscape shifts. [8]

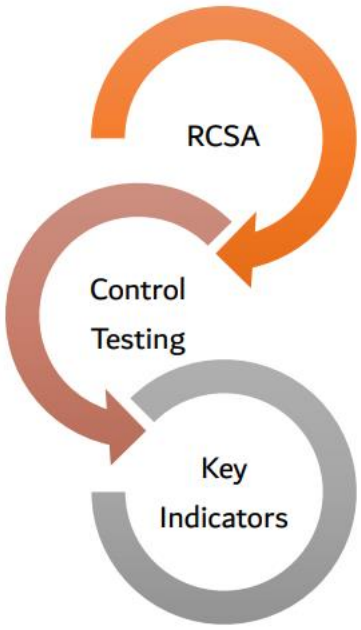


Figure 1. 5 : RCSA path to the next step

1.7.3 What Does Risk Control Include?

Also known as “risk treatment,” risk control includes the following.

- **Risk avoidance**. Applying safeguards that eliminate or reduce the business risks that can harm the organization’s assets. While risk management seeks to control the damages and financial consequences of threats, risk avoidance aims to avoid the threats entirely.

- **Risk transference**. Shifting the risk to other areas of the business or to outside entities, such as an insurance company. The goal here is to let another entity accept the risk. For example, a company could outsource business processes as data storage or IT management, transferring the risk to providers of those services (under the logic that they are experts in those fields, better able to handle the risk).

- **Risk mitigation.** Reducing the impact if a bad actor exploits a vulnerability. Risk mitigation means having policies and procedures in place to lessen the adverse effects when something happens. These risk mitigation strategies include incident response plans, disaster recovery plans, and business continuity plans.

- **Risk acceptance**. Understanding the potential consequences of a risk, and accepting the chance of those consequences without control or mitigation. An organization might do this when it believes the chance of the risk happening is minimal, or the potential harm from the risk wouldn't be significant. [8]

1.7.4 Example Of Risk Control

As part of Sumitomo Electric's risk management efforts, the company developed business continuity plans (BCPs) in fiscal 2008 as a means of ensuring that core business activities could continue in the event of a disaster. The BCPs played a role in responding to issues caused by the Great East Japan earthquake that occurred in March 2011. Because the quake caused massive damage on an unprecedented scale, far surpassing the damage assumed in the BCPs, some areas of the plans did not reach their goals.

Based on lessons learned from the company's response to the earthquake, executives continue promoting practical drills and training programs, confirming the effectiveness of the plans and improving them as needed. In addition, Sumitomo continues setting up a system for coping with risks such as outbreaks of infectious diseases, including the pandemic influenza virus. [8]

1.7.5 What is Risk Control and Self Assessment (RCSA)?

The risk control and self-assessment (RCSA) methodology have certain characteristic features.

It is important to know that this process is dynamic. This means that it keeps changing constantly and depends upon the level of controls which have been introduced by the unit.

The risk control and self-assessment (RCSA) is iterative in nature. This means that the methodology works on a trial and error basis. Whenever any measure is taken to monitor risks, the effect is constantly measured. If the solution is not working as intended, the process is changed and the iteration is repeated

The risk control and self-assessment (RCSA) process does not take place at the organization level. Instead, as a part of this process, organizational units are identified. The policies are implemented and the success is monitored at the unit level. The organization-wide risk control and self-assessment (RCSA) is just the sum of the different units in the company

1.7.6 Steps Followed During Risk Control and Self Assessment (RCSA)

The risk control and self-assessment (RCSA) methodology is a structured methodology that has four different stages. One stage may have one or more steps. The details regarding these stages have been mentioned below: [8]

1.7.6.1 Stage 1: Documentation and Definition

The first step in the process is to identify and define organizational units for the purpose of risk management. These units need to be structured in the form of a hierarchy. The end result of the exercise is that the risk entities are identified and also the relationship between them is clearly defined. These reporting relationships also need to be defined so that data from individual risk entities can be combined to develop the organizational risk profile. This is the stage at which the companies generally do their top-down analysis for identifying operational risks. The documentation of control procedures as well as how they relate to operational risks is also extremely important. At this stage, the company does not actually pay attention to the risks and their mitigation. The focus is on identifying and documenting the control structure.

1.7.6.2 Stage 2: Identification of Risks

The second stage is where the identification of risks happens. This is generally done in three steps. The first step is to identify the risks which emanate from the top-level entity. Since these risks are from a higher level, they apply to all the

organizational units within the entity. The next step includes the regulatory risks which arise from government policies and interactions with regulators. Lastly, unit-wise additional risks are taken into account in order to correctly understand the risk profile of a particular unit. The last step in the process is to categorize risks. This is done by assigning a monetary value to the risk and recognizing its severity.

1.7.6.3 Stage 3: Assessment of Controls

In this step, the risks are divided into categories. Controls and risk mitigation plans are set up for materialistic risks. Each entity is responsible for managing its own risks and developing an action plan. Risk entities are supposed to have multiple plans in place. This is because if a particular plan does not work, then it can be replaced with a different plan. It is important to note that this process is continuous and must be done periodically. Risk controls that are effective today may not remain effective after a certain period of time. As a part of this process, companies also have to set up methods that will help use samples to determine the effectiveness of the plans. The manner in which samples have to be selected as well as the interpretation of results has to be defined at this stage.

1.7.6.4 Stage 4: Reviews and Ratings

At the end of the exercise, the mitigation plans are also categorized. Common categories are used as acceptable, less than acceptable, and acceptable with concerns. This categorization is derived from the scores generated in the previous stage. Since this exercise is conducted periodically, it would be prudent to ensure that this score is actually an average of the past few scores. This would represent the risk on a continuum instead of presenting it in a static manner. based on the ratings, the organizations can decide to implement secondary plans, and then the process repeats itself. The end result of this process is that risk entities are constantly engaged in risk management activity. In many organizations, a dashboard is maintained where the risk levels of various units are constantly monitored. Thus the risk control and self-assessment (RCSA) framework helps in mitigating operational risks.

1.8 Key Risk Indicators

1.8.1 What are Key Risk Indicators?

In simple words, key risk indicators can be understood to be predictors of adverse events which are likely to impact organizations. Organizations are impacted when their environment changes. Hence, if the changes in the environment are continuously monitored then the changes in the risk exposure can be spotted early. This would help organizations to identify, report and manage risks better than other companies. The best way to think about the key risk indicators is to think about them as the dashboard of a car. The dashboard conveys important information which must be tracked numerically in order to ensure the smooth functioning of the organization from an operational risk point of view.[9]



Figure 1. 6 : Key Operational Risk Indicator

The main feature of the key risk indicator is that it should be expressed numerically. This also means that there should be a predefined level for these numbers and then when they vary from the predefined level, they should be immediately reported to the risk management team. [9]

1.8.2 Designing the Key Risk Indicators

Key risk indicators can be considered to be the lens through which the company views its internal and external environment. This means that choosing the key risk indicators correctly is of utmost importance while designing the risk management system.

The designing of key risk indicators is quite complex since it requires an understanding of the various objectives of the organization as well as the environmental factors which can hinder the achievement of these organizational goals.

The first step in designing a key risk indicator is to understand the cause-effect relationship between the organization's goals and some root cause factors. The next step is to understand the relative significance that each of these root cause factors has on the overall achievement of the goals. The next step is to create a system that collects high-quality data about these indicators. The data collected must be genuine and there must not be too much time lag between the collection of the data and the passing of this data to the risk management decision-making process.

Also, it is important to ensure that only meaningful indicators are incorporated into the key performance indicator process. If too many metrics are simultaneously tracked, it dilutes focus and the company is not able to pay attention to what is really important. It is also important to determine the trigger levels of the key risk indicators in accordance with the risk appetite of the company that has been aligned during the creation of the risk policy. [9]

1.8.3 Difference Between KRIs and KPIs

Key performance indicators or KPIs are also tools that are used by organizations to manage their day-to-day operations. For instance, revenue being generated, costs being incurred, etc are examples of key performance indicators. However, key performance indicators are not the same as key risk indicators.

Key risk indicators can be thought of as being the precursor to the key performance indicators. The objective of the company is to ensure that the performance indicators are never affected. This is the reason that a separate set of indicators called the key risk indicators are used. The effect of the risk should ideally be shown first in the risk indicators before it starts showing up in performance indicators. If that is not the case, then the system has been designed poorly. [9]

1.8.4 Key Control Indicators

An effective operational risk management system also has key control indicators in place. These indicators help an organization determine the success of its key risk indicators. If the risk indicators are able to catch risks early and maintain control over the operational performance, then that will be reflected in the key control indicators. Key control indicators help a company decide whether its risk indicators are accurate or whether they need to be changed. [9]

1.8.5 Challenges of Key Risk Indicators

The key risk indicator model is not free from challenges. Some of the commonly faced challenges have been mentioned below:

It may be difficult to identify the key risk indicators for all risks which are faced by an organization. This is because there are certain unknown risks that the organization is not even aware of. It may be difficult to build an automatic system that collects the values and intimates the decision-makers at the correct time. It is also possible that companies may focus too much on the symptoms of the key risk indicators instead of focusing on the actual root cause. Lastly, many companies may not have action plans ready. There may be ambiguity about the actions that need to be taken once an action crosses a certain threshold. The bottom line is that the key risk indicator model is an integral part of the advanced measurement model suggested in the Basel norms. This is the reason that this model is followed widely in different parts of the world. [9]

1.9 Action Plans

1.9.1 What is a Risk action plan?

A risk action plan is the course of action which an organisation agrees upon to help them to address potential risks, reduce the likelihood of these risks occurring and to lessen the impact of these risks if they do occur. A plan is created to ensure that the right actions are carried out in a timely manner. A plan also provides a go-to guide, in case the “unexpected” happens.

1.9.2 What is the purpose of a Risk action plan?

A risk action plan helps to prepare you to face potential risks which may occur as part of a business scenario and helps you to tackle any problems with may occur. A risk action plan will provide you with strategies which are appropriate dependent on the levels of risk which your organisation faces.

1.9.3 What are the different types of Risk action plans?

1.9.3.1 Risk Avoidance Plans

These plans include measures which aim to completely avoid the risks in question by preventing them from happening.

1.9.3.2 Risk Reduction Plans

These plans include measures which reduce the likelihood of a risk occurring or reduce the effects of a risk if it does occur.

1.9.4 Where does a Risk action plan fit into the risk management process?

Creating a risk action plan comes at the middle of the risk management process, between evaluation of risks and before the monitoring process.

1.10 The Followed model

Advanced measurement model (AMM) is one of three possible operational risk methods that can be used under Basel II by a bank or other financial institution. The other two are the Basic Indicator Model and the Standardised Model. The methods (or modeles) increase in sophistication and risk sensitivity with AMM being the most advanced of the three. Under AMM the banks are allowed to develop their own empirical model to quantify required capital for operational risk. Banks can use this model only subject to approval from their local regulators. Once a bank has been approved to adopt AMM, it cannot revert to a simpler model without supervisory approval.

The global financial crisis of the past decade contributed to increasing the awareness of the banking institutions regarding the importance of good risk management.

The multitude of factors that can generate the risk and the financial losses that it can bring to a credit institution, have led to the introduction of the operational risk (and its sub-categories) in the category of the three most important risks in the banking activity, beside the credit risk and market risk. In the last 15 years, numerous regulations for operational risk management have been elaborated, the most important of these being the Basel II Agreement, whereby credit institutions are obligated to calculate the minimum capital requirements for operational risks,using 3 calculation methods, proposed within the same agreement:

- Basic Indicator Model – BIM
- Standardized Model - SM and Advanced
- Measurement Model - AMM.

Chapter 2
technologies & system implementation

2 Chapter 2: technologies & system implementation

2.1 Introduction

This chapter provides a tour of main software development methods, librariesand patterns and their assimilation with usability, various methods have been developed since the appearance of software products.

Researchers were also keen to integrate usability with these methods to develop a successful and resilient applications and achieve a great height that might not lose itsgrip over their competitors.

Walking through the footprints marked by these mentors, the proposed ORM solution extracted the pulp of each robust method in which related primary keys have beengathered and described in the coming sections.

2.2 Site Rendering

To begin this journey, we need to understand the concept of site rendering. In layman's terms, siterendering means generating or rendering HTML output. HTML is a markup language that web developers use to create web pages. It's said that site rendering can happen both at server-side or client-side level, so what does this mean? It's worth noting that frontend and client-side are synonyms. The same is true for backend and server-side.

2.3 Server-Side Rendering (Backend)

Not until too long ago, server-side rendering, or back-end web development, was the de facto wayto create websites and web applications. You visit a page, send a request for content, the server processes this request and creates a response that is sent back to your browser.

When a site renders server-side, all the processes involved in creating an HTML page that your web browser can understand are handled on a remote server hosting the website or web application.This includes querying databases for information and processing any logic that your web application requires.

While the remote server is busy at work, your web browser is idle, waiting for the server to finishprocessing the request and sending a response. When the response is received, web browsers interpret it and display the content on the screen.

2.4 Client-Side Rendering (frontend)

In more modern days, a new form of site rendering emerged called client-side rendering or front- end development.

With client-side rendering, the rendering of the content happens in your computer instead of the remote web server using the de facto language of the web, JavaScript. In practical terms, it meansthat a server is only needed to serve the raw web application, and the browser will be in charge ofrendering this application in its final form, HTML. It also means that some of the logic involved increating the web page, especially the one in charge of dealing with how things are presented to theuser on the screen (called presentation logic) are handled on the client-side. Client-side rendering became popular with the advent of JavaScript libraries such as Angular, Reactand Vue.

2.5 Technologies used for backend development

When back-end developers create apps that render on the server-side, they use the same building blocks as front-end developers: HTML, CSS and JavaScript. Back-end developers also work with software stacks that include operating systems, web servers, frameworks, languages, programming APIs and more. The frameworks, languages andprogramming APIs in these stacks are used to render server-side sites and web applications and tocreate services that other applications can consume. Notorious stacks include .NET, Spring and LAMP, but there are many more, and each includes a programming language of choice, such as C#, JavaScript, Java, Go, Python or PHP.

2.6 Technologies used for backend development

While there are many different types of technologies and stacks, most front-end web developers use HTML, CSS and JavaScript, the de facto building blocks of the web, and client-side frameworks such as Angular, React, Stencil and Vue. Not everything happens on the frontend, though. Client-side rendered applications still rely on services and APIs that run on back-end remote servers or the cloud.

2.7 BACKEND With Java Spring Boot

Spring Boot is an open source Java-based framework used to create a microService. It is developed by Pivotal Team and is used to build stand-alone and production ready spring applications. This chapter will give you an introduction to Spring Boot and familiarizes you with its basic concepts.

2.7.1 What is Micro Service?

Micro Service is an architecture that allows the developers to develop and deploy services independently. Each service running has its own process and this achieves the lightweight model to support business applications.[10]

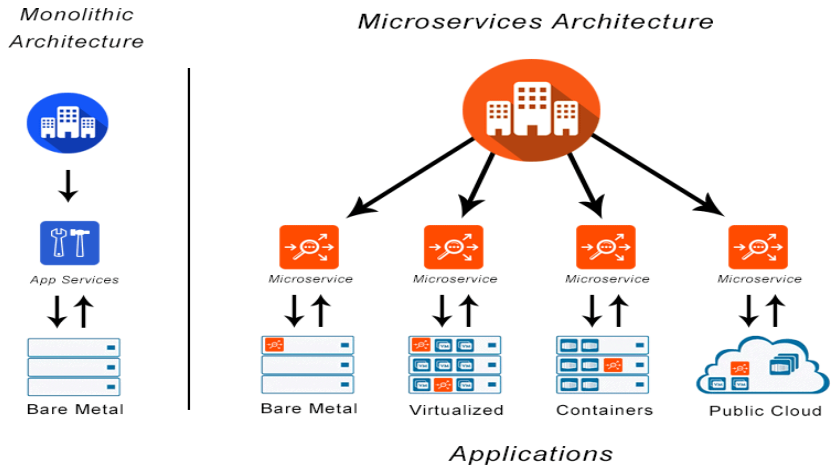


Figure 2. 1 : Microservices vs Monolithic architecture

2.7.2 Advantages

Micro services offer the following advantages to its developers:

- Easy deployment
- Simple scalability
- Compatible with Containers
- Minimum configuration
- Lesser production time

2.7.3 What is Spring Boot?

Spring Boot provides a good platform for Java developers to develop a stand-alone and production-grade spring application that you can **just run**. You can get started with minimum configurations without the need for an entire Spring configuration setup.[11]

2.7.4 Advantages

Spring Boot offers the following advantages to its developers :

- Easy to understand and develop spring applications
- Increases productivity
- Reduces the development time . [11]

2.7.5 Goals

Spring Boot is designed with the following goals :

- To avoid complex XML configuration in Spring
- To develop a production ready Spring applications in an easier way
- To reduce the development time and run the application independently
- Offer an easier way of getting started with the application. [11]

2.7.6 Why Spring Boot?

You can choose Spring Boot because of the features and benefits it offers as givenhere −

- It provides a flexible way to configure Java Beans, XML configurations, andDatabase Transactions.
- It provides a powerful batch processing and manages REST endpoints.
- In Spring Boot, everything is auto configured; no manual configurations areneeded.
- It offers annotation-based spring application
- Eases dependency management
- It includes Embedded Servlet Container. [11]

2.7.7 How does it work?

Spring Boot automatically configures your application based on the dependencies you haveadded to the project by using **@EnableAutoConfiguration** annotation. For example, if MySQLdatabase is on your classpath, but you have not configured any database connection, then Spring Boot auto-configures an in-memory database.

The entry point of the spring boot application is the class contains @SpringBootApplication annotation and the main method.

Spring Boot automatically scans all the components included in the project byusing **@ComponentScan** annotation. [11]

2.7.8 Spring Boot Starters

Handling dependency management is a difficult task for big projects. Spring Boot resolves thisproblem by providing a set of dependencies for developers convenience.

For example, if you want to use Spring and JPA for database access, it is sufficient if youinclude **spring-boot-starter-data-jpa** dependency in your project.

Note that all Spring Boot starters follow the same naming pattern **spring-boot-starter-***, where

* indicates that it is a type of the application. [11]

2.7.8.1 Examples

Look at the following Spring Boot starters explained below for a better understanding −

Spring Boot Starter Actuator dependency is used to monitor and manage your application. Itscode is shown below :

```
<dependency>
   <groupId>org.springframework.boot</groupId>
   <artifactId>spring-boot-starter-actuator</artifactId>
</dependency>
```

Spring Boot Starter Security dependency is used for Spring Security. Its code is shown below :

```
<dependency>
   <groupId>org.springframework.boot</groupId>
   <artifactId>spring-boot-starter-security</artifactId>
</dependency>
```

Spring Boot Starter web dependency is used to write a Rest Endpoints. Its code is shown below :

```
<dependency>
   <groupId>org.springframework.boot</groupId>
   <artifactId>spring-boot-starter-web</artifactId>
</dependency>
```

Spring Boot Starter Thyme Leaf dependency is used to create a web application. Its code isshown below :

```
<dependency>
   <groupId>org.springframework.boot</groupId>
   <artifactId>spring-boot-starter-thymeleaf</artifactId>
</dependency>
```

Spring Boot Starter Test dependency is used for writing Test cases. Its code is shown below :

```
<dependency>
   <groupId>org.springframework.boot</groupId>
   <artifactId>spring-boot-starter-test</artifactId>
</dependency>
```

2.7.9 Auto Configuration

Spring Boot Auto Configuration automatically configures your Spring application based on the JAR dependencies you added in the project. For example, if MySQL database is on your class path, but you have not configured any database connection, then Spring Boot auto configuresan in-memory database. [11]

For this purpose, you need to add **@EnableAutoConfiguration** annotationor **@SpringBootApplication** annotation to your main class file. Then, your Spring Boot application will be automatically configured.

Observe the following code for a better understanding :

```
import org.springframework.boot.SpringApplication;
import
org.springframework.boot.autoconfigure.EnableAutoConfiguration;

@EnableAutoConfiguration
public class DemoApplication {
   public static void main(String[] args) {
      SpringApplication.run(DemoApplication.class, args);
   }
}
```

2.7.10 Spring Boot Application

The entry point of the Spring Boot Application is the class contains **@SpringBootApplication** annotation. This class should have the main method to run the SpringBoot application. **@SpringBootApplication** annotation includes Auto- Configuration,Component Scan, and Spring Boot Configuration.

If you added **@SpringBootApplication** annotation to the class, you do not need to addthe **@EnableAutoConfiguration, @ComponentScan** and **@SpringBootConfiguration** annotation. The **@SpringBootApplication** annotation includes all other annotations.

Observe the following code for a better understanding :

```
import org.springframework.boot.SpringApplication;
import org.springframework.boot.autoconfigure.SpringBootApplication;

@SpringBootApplication
public class DemoApplication {
   public static void main(String[] args) {
      SpringApplication.run(DemoApplication.class, args);
   }
}
```

2.7.11 Component Scan

Spring Boot application scans all the beans and package declarations when the applicationinitializes. You need to add the **@ComponentScan** annotation for your class file to scan your components added in your project.

Observe the following code for a better understanding :

```
import org.springframework.boot.SpringApplication;
import org.springframework.context.annotation.ComponentScan;

@ComponentScan
public class DemoApplication {
   public static void main(String[] args) {
      SpringApplication.run(DemoApplication.class, args);
   }
}
```

2.8 What is an API?

An **API** is a set of programming code that enables data transmission between one softwareproduct and another. It also contains the terms of this data exchange.

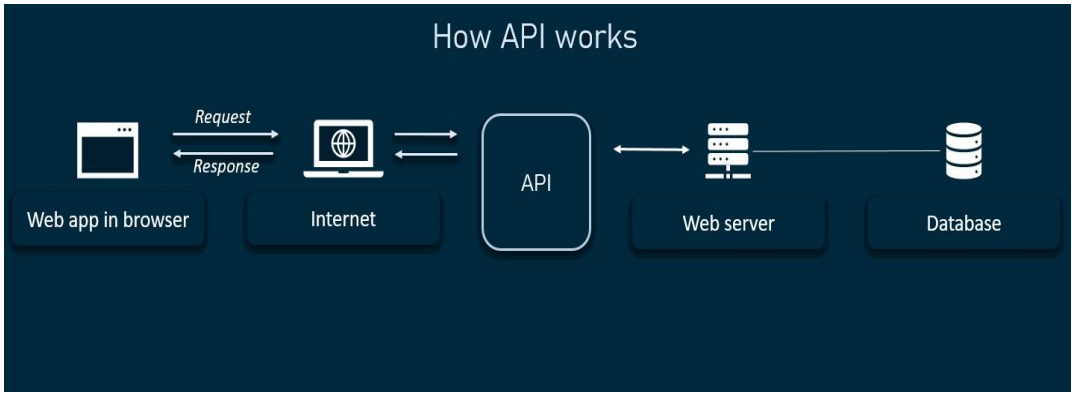


Figure 2. 2 : How Api Work

Application programming interfaces consist of two components:

- Technical specification describing the data exchange options between solutions with thespecification done in the form of a request for processing and data delivery protocols
- Software interface written to the specification that represents it

The software that needs to access information (i.e., X hotel room rates for certain dates) or functionality (i.e., a route from point A to point B on a map based on a user's location) from anothersoftware, calls its API while specifying the requirements of how data/functionality must be provided. The other software returns data/functionality requested by the former application.And the interface by which these two applications communicate is what the API specifies.[12]

Each API contains and is implemented by **function calls** – language statements that request software to perform particular actions and services. Function calls are phrases composed of verbs and nouns,

for example:

- Start or finish a session
- Get amenities for a single room type
- Restore or retrieve objects from a server.

2.8.1 Types of APIs

In terms of release policies, APIs can be private, partner, and public.

Private APIs. These application software interfaces are designed for improving solutions and services within an organization. In-house developers or contractors may use these APIs to integratea company's IT systems or applications, build new systems or customer-facing apps leveraging existing systems. Even if apps are publicly available, the interface itself remains available only forthose working directly with the API publisher. The private strategy allows a company to fully control the API usage.

Partner APIs. Partner APIs are openly promoted but shared with business partners who have signed an agreement with the publisher. The common use case for partner APIs is software integration between two parties. A company that grants partners with access to data or capability benefits from extra revenue streams. At the same time, it can monitor how the exposed digital assets are used, ensure whether third-party solutions using their APIs provide decent user experience, and maintain corporate identity in their apps. [12]

Public APIs. Also known as developer-facing or external, these APIs are available for any third- party developers. A public API program allows for increasing brand awareness and receiving an additional source of income when properly executed. [12]

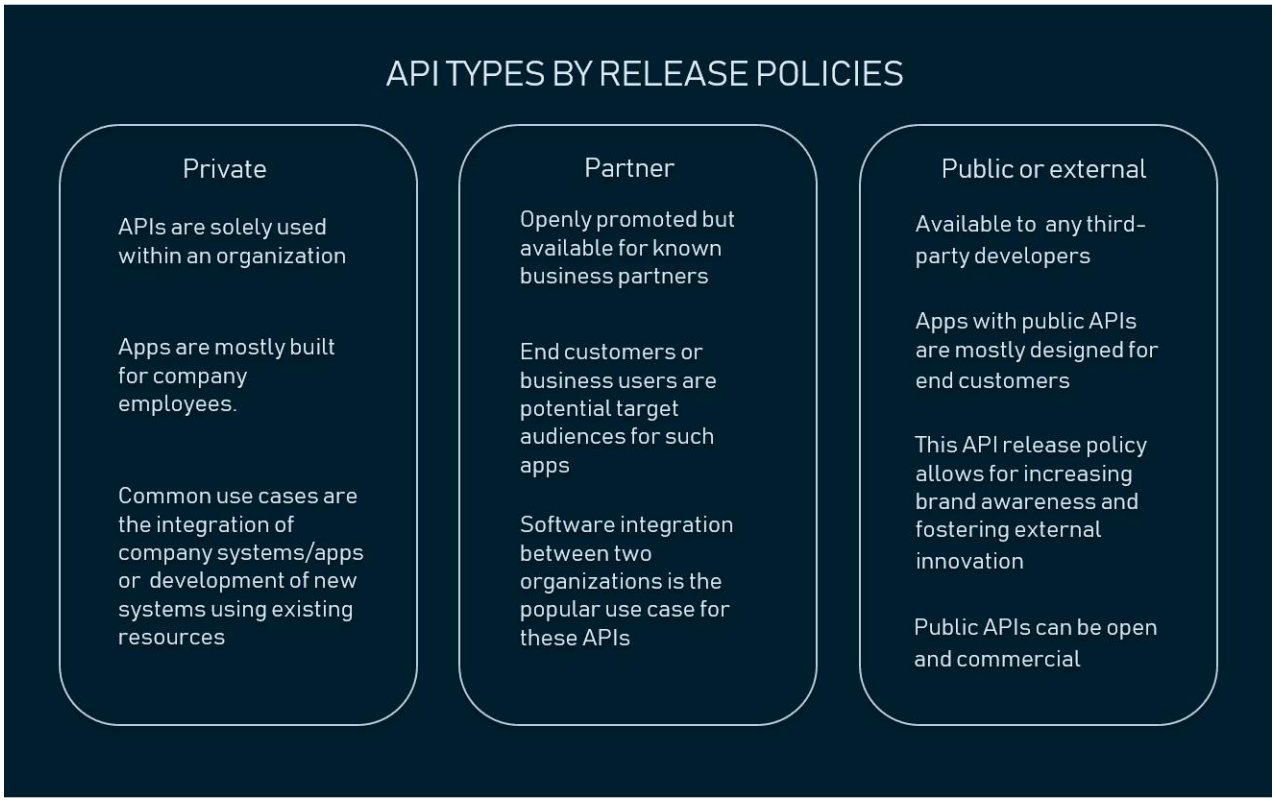


Figure 2. 3:API Types by release Policies

2.8.2 Design Patterns

a **design pattern** is a general repeatable solution to a commonly occurring problem in software design. A design pattern isn't a finished design that can be transformed directly into code.It is a description or template for how to solve a problem that can be used in many different situations.[13]

2.8.3 Design Patterns used in Spring Framework

Design Pattern	Details
MVC Pattern	MVC Design Pattern is a software design that separates the following components of a system or subsystem: • **Model -** Data about the state of the application or its components. May include routines for modification or access. • **View -** An interpretation of the data (model). This is only limited to a visual representation, but could be audio, derived information (e.g. statistics piped into another model object), etc. Furthermore, a single model may have multiple views. • **Control -** Handles external input to the system invoking modifications on the model. The control/view may be closely related (in the case of a UI). However, other external input (such as network commands), may be processed which are completely independent of the view.
Proxy Pattern	Spring uses either JDK proxies (preferred wheneven the proxied target implements at least one interface) or CGLIB proxies (if the target object does not implement any interfaces) to create the proxy for a given target bean. Unless configured to do otherwise, Spring AOP performs run-time weaving Suppose we want to log every method entry and exit. This can be achieved by writing log statements in every method at the start and end. But this will require lot of code work. There are various such tasks like Security which need to be applied across all methods or classes. These are known as cross cutting concerns.AOP addresses the problem of cross-cutting concerns, which would be any kind of code that is repeated in different methods and cannot normally be completely refactored into its own module, like with logging or verification.
Factory Pattern	This patterns is used by spring to load beans using BeanFactory and Application context.
Singleton Pattern	Beans defined in spring config files are singletons by default. A singleton bean in Spring and the singleton pattern are quite different. Singleton pattern says that one and only one instance of a particular class will ever be created per classloader. The scope of a Spring singleton is described as "per container per bean". It is the scope of bean definition to a single object instance per Spring IoC container. The default scope in Spring is Singleton. [14]

Template method Pattern	Template method design pattern is to define an algorithm as skeleton of operations and leave the details to be implemented by the child classes. The overall structure and sequence of the algorithm is preserved by the parent class. These are used extensively to deal with boilerplate repeated code
FrontController Pattern	Front Controller is a controller pattern which provides a centralized controller for managing requests. Each client request must go through and be processed by the Front Controller first, no exceptions. All incoming data is delegated to front controller first. Useful for when your application has multiple entry points which you want to centralize through a single point for standardized processing. Spring implements this design pattern using DispatcherServlet, to dispatch incoming requests to the correct controllers.
View Helper Pattern	View Helper arranges view components for the user and delegates processing to other business components so the view component doesn't have to contain any processing logic other than logic to present views. Spring makes use of custom JSP tags etc to separate code from presentation in views.
Prototype Pattern	The Prototype pattern is known as a creational pattern,as it is used to construct objects such that they can be decoupled from their implementing systems. It creates objects based on a template of an exsiting object through cloning.
DI/IOC Pattern	Dependency Injection/Inversion of Control design pattern allows us to remove the hard-coded dependencies and make our application loosely coupled, extendable and maintainable. We can implement dependency injection in java to move the dependency resolution from compile-time to runtime.[14]

2.8.4 What Is Hibernate in Spring Boot

Hibernate **understands the mappings that we add between objects and tables**. It ensuresthat data is stored/retrieved from the database based on the mappings. Hibernate also provides additional features on top of JPA. But depending on them would mean a lock in to Hibernate.[15]

2.8.5 How does JPA/Hibernate Work?

Databases are designed with Tables/Relations. Java objects are designed using OOPS. Developers would want to store the data from objects into tables and vice-versa. Earlier modeles involved writing SQL Queries. JDBC, Spring JDBC and myBatis were popular modeles. However, JPA evolved as a result of a different thought process. But how about mapping the objects directly to tables/relationships? This Mapping is also called ORM - Object Relational Mapping. Before JPA, ORM was the term more commonly used to refer to these frameworks. That's one of the reasons, Hibernate is called aORM framework. [15]

2.8.6 Important Concepts in JPA

JPA allows to map application classes to tables in database.

- Entity Manager - Once the mappings are defined, entity manager can manage your entities.Entity Manager handles all interactions with the database
- JPQL (Java Persistence Query Language) - Provides ways to write queries to execute searches against entities. Important thing to understand is the these are different from SQLqueries. JPQL queries already understand the mappings that are defined between entities. We can add additional conditions as needed.
- Criteria API defines a Java based API to execute searches against databases. [15]

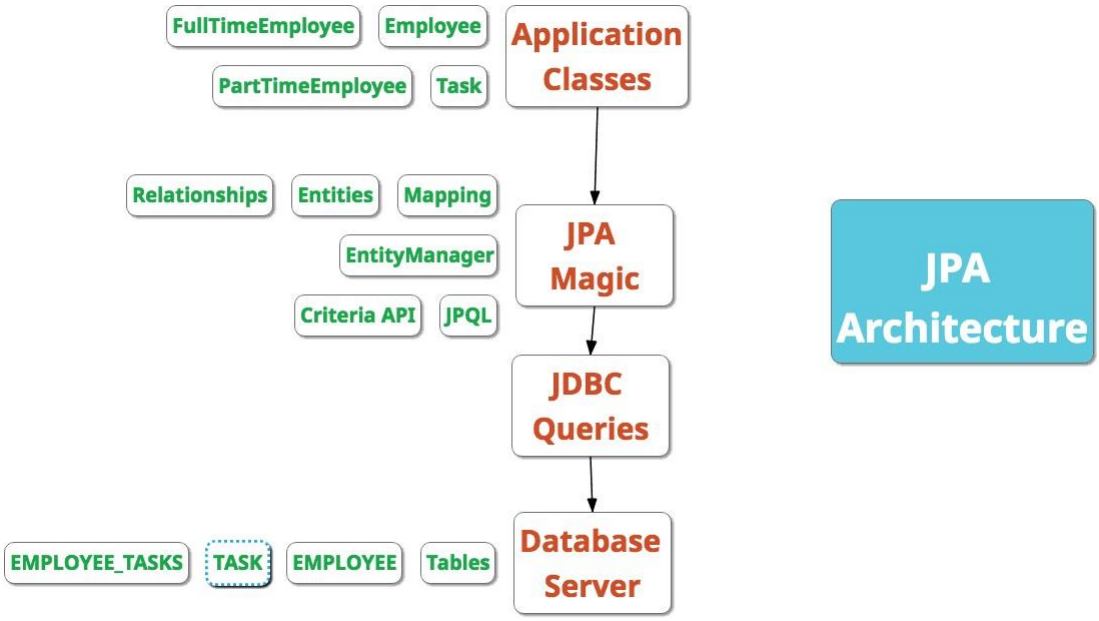


Figure 2. 4 : JPA Architecture

2.8.7 JPA vs Hibernate

Like already mentioned Hibernate is one of the most popular ORM frameworks.JPA defines the specification. It is an API.

- How do you define entities?
- How do you map attributes?
- How do you map relationships between entities?
- Who manages the entities?

Hibernate is one of the popular implementations of JPA.

- Hibernate understands the mappings that we add between objects and tables. It ensuresthat data is stored/retrieved from the database based on the mappings.
- Hibernate also provides additional features on top of JPA. But depending on them wouldmean a lock in to Hibernate. You cannot move to other JPA implementations like Toplink. [15]

2.9 JavaMail

The **JavaMail** is an API that is used to compose, write and read electronic messages(emails). The JavaMail API provides protocol-independent and plateform-independent framework for sending and receiving mails.

The **javax.mail** and **javax.mail.activation** packages contains the core classes of JavaMail API.

The JavaMail facility can be applied to many events. It can be used at the time of registering the user (sending notification such as thanks for your interest to my site), forgot password (sending password to the users email id), sending notifications for important updates etc. So there can be various usage of java mail api.

2.9.1 Protocols used in JavaMail API

There are some protocols that are used in JavaMail API.

SMTP: SMTP is an acronym for Simple Mail Transfer Protocol. It provides a mechanism to deliverthe email. We can use Apache James server, Postcast server, cmail server etc. as an SMTP server.But if we purchase the host space, an SMTP server is by default provided by the host provider. Forexample, my smtp server is mail.javatpoint.com. If we use the SMTP server provided by the host provider, authentication is required for sending and receiving emails.

POP: POP is an acronym for Post Office Protocol, also known as POP3. It provides a mechanismto receive the email. It provides support for single mail box for each user. We can use Apache James server, cmail server etc. as a POP server. But if we purchase the host space, a POP server isby default provided by the host provider. For example, the pop server provided by the host providerfor my site is mail.javatpoint.com. This protocol is defined in RFC 1939.

IMAP: IMAP is an acronym for Internet Message Access Protocol. IMAP is an advanced protocolfor receiving messages. It provides support for multiple mail box for each user, in addition to, mailbox can be shared by multiple users. It is defined in RFC 2060.

2.9.2 JavaMail Architecture

The java application uses JavaMail API to compose, send and receive emails. The JavaMailAPI uses SPI (Service Provider Interfaces) that provides the intermediatory services to the java application to deal with the different protocols. Let's understand it with the figure given below:

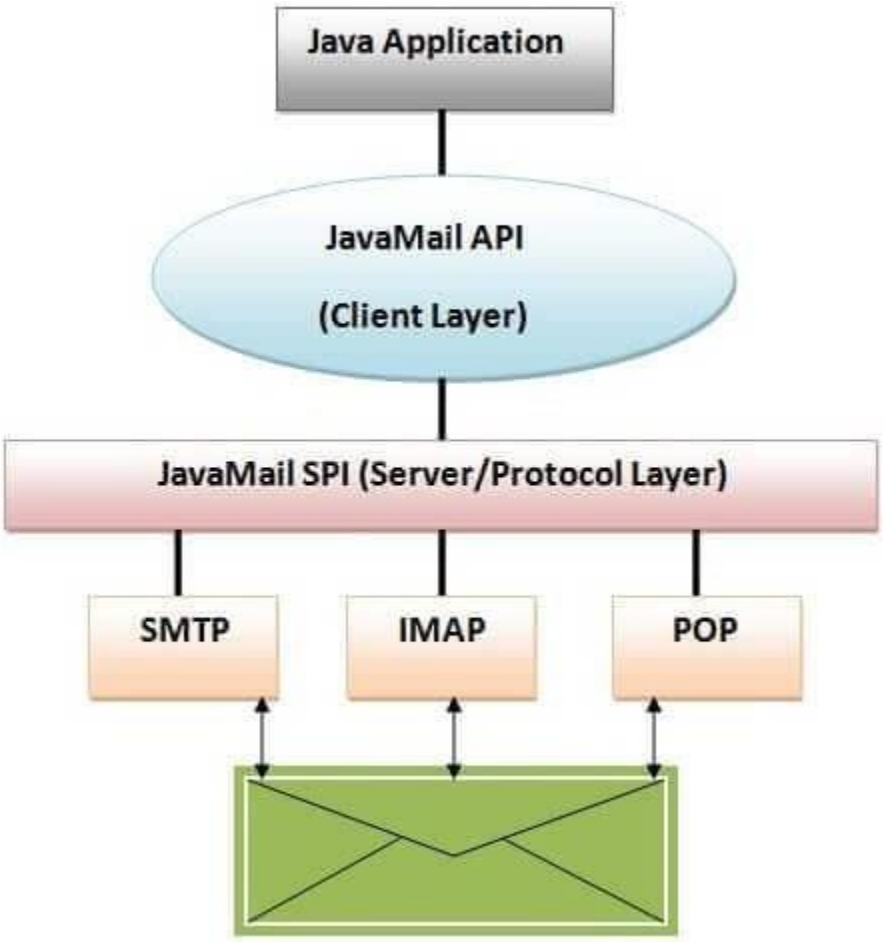


Figure 2. 5 : JavaMail Architecture

2.9.3 Java Mail API in Spring Boot

The interfaces and classes for java mail support in spring framework are as follows:

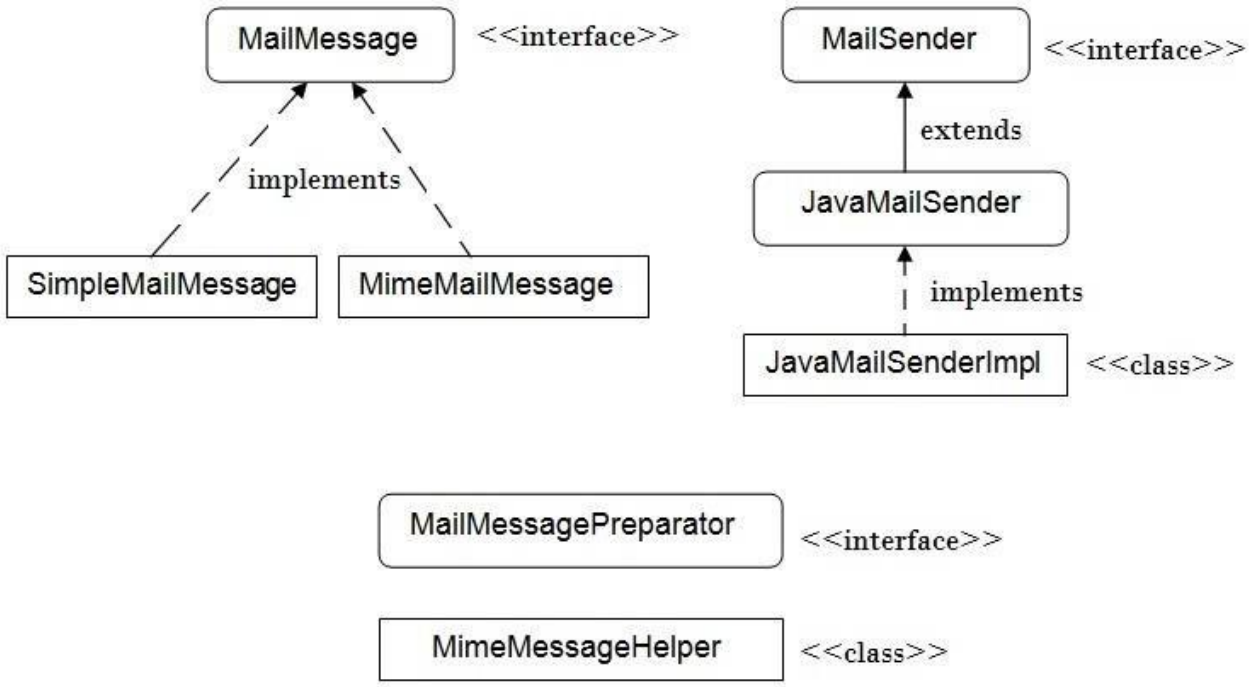


Figure 2. 6 : java mail support in spring framework

2.10 What is Redis Cache?

Redis is short for Remote Dictionary Server. Redis is a caching system that works by temporarilystoring information in a key-value data structure.

Redis cache is popular because it is available in almost all major programming languages. In addition, like WordPress, it is open source, which means it is a well-supported system that is a brilliant way to speed up your website or application without incurring a high cost. [16]

2.10.1 What is Redis used for?

Redis is used for speeding up website page load time for users. When it comes to the proposed ORM application, it is mainly used as a caching system to temporarily store information that wouldusually sit in a database. This way, it can be loaded much faster rather than having to access the database directly.[17]

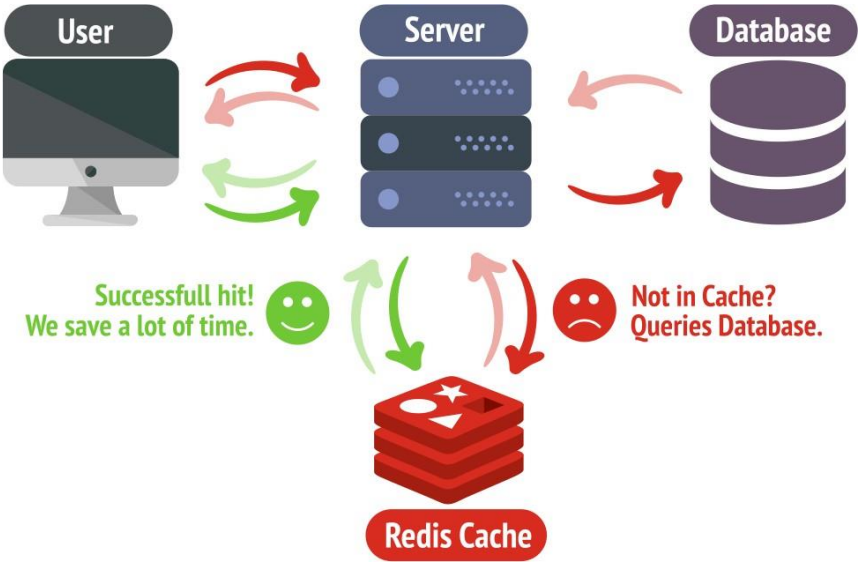


Figure 2. 7 : how Redis is used

2.11 Spring Boot Security with Oauth2-JWT

the coming section will cover how the security aspect is implemented and that by introducing:

Authorization Server: Authorization Server is a supreme architectural component for WebAPI Security. The Authorization Server acts a centralization authorization point that allows your apps and HTTP endpoints to identify the features of your application.

Resource Server: Resource Server is an application that provides the access token to the clients to access the Resource Server HTTP Endpoints. It is collection of libraries which contains the HTTP Endpoints, static resources, and Dynamic web pages.

OAuth2: OAuth2 is an authorization framework that enables the application Web Security to access the resources from the client. To build an OAuth2 application, we need to focus on the GrantType (Authorization code), Client ID and Client secret.

JWT: JSON Web Token (JWT) is an open standard that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information canbe verified and trusted because it is digitally signed. JWTs can be signed using a secret (with the HMAC algorithm) or a public/private key pair using RSA or ECDSA.

2.12 Frontend With Angular:

Angular is a development platform, built on TypeScript As a platform, Angular includes:

- A component-based framework for building scalable web applications
- A collection of well-integrated libraries that cover a wide variety of features, includingrouting, forms management, client-server communication, and more
- A suite of developer tools to help you develop, build, test, and update your code

With Angular, developers are taking advantage of a platform that can scale from single-developerprojects to enterprise-level applications. Angular is designed to make updating as straightforward as possible, so take advantage of the latest developments with a minimum of effort. Best of all, theAngular ecosystem consists of a diverse group of over 1.7 million developers, library authors, andcontent creators.[18]

2.12.1 Angular Essentials and Architecture

The architecture of an Angular application relies on certain fundamental concepts. The basic building blocks of the Angular framework are Angular components that are organizedinto *NgModules*. NgModules collect related code into functional sets; an Angular application is defined by a set of NgModules. An application always has at least a *root module* that enables bootstrapping, and typically has many more *feature modules*.

- Components define *views*, which are sets of screen elements that Angular can choose among and modify according to your program logic and data
- Components use *services*, which provide specific functionality not directly related to views.Service providers can be *injected* into components as *dependencies*, making your code modular, reusable, and efficient.

Modules, components and services are classes that use *decorators*. These decorators mark their type and provide metadata that tells Angular how to use them.

- The metadata for a component class associates it with a *template* that defines a view. A template combines ordinary HTML with Angular *directives* and *binding markup* that allowAngular to modify the HTML before rendering it for display.
- The metadata for a service class provides the information Angular needs to make it available to components through *dependency injection (DI)*

An application's components typically define many views, arranged hierarchically. Angular provides the Router service to help you define navigation paths among views. The router providessophisticated in-browser navigational capabilities. [18]

2.12.2 Modules

An NgModule declares a compilation context for a set of components that is dedicated to an application domain, a workflow, or a closely related set of capabilities. An NgModule can associateits components with related code, such as services, to form functional units.

Every Angular application has a *root module*, conventionally named AppModule, which providesthe bootstrap mechanism that launches the application. An application typically contains many functional modules.

NgModules can import functionality from other NgModules, and allow their own functionality tobe exported and used by other NgModules. For example, to use the router service in your app, youimport the Router NgModule. [18]

2.12.3 Components

Every Angular application has at least one component, the *root component* that connects a component hierarchy with the page document object model (DOM). Each component defines a class that contains application data and logic, and is associated with an HTML *template* that definesa view to be displayed in a target environment.

The @Component() decorator identifies the class immediately below it as a component, and provides the template and related component-specific metadata. [18].

2.12.4 Templates, Directives and Data binding

A template combines HTML with Angular markup that can modify HTML elements before they are displayed. Template *directives* provide program logic, and *binding markup* connects yourapplication data and the DOM. There are two types of data binding:

DATA BINDINGS	DETAILS
Event binding	Lets your application respond to user input in the target environment by updating your application data.
Property binding	Lets you interpolate values that are computed from your application data into the HTML.

Before a view is displayed, Angular evaluates the directives and resolves the binding syntax in thetemplate to modify the HTML elements and the DOM, according to your program data and logic.Angular supports *two-way data binding*, meaning that changes in the DOM, such as user choices,are also reflected in The program data.

The templates can use *pipes* to improve the user experience by transforming values for display. Forexample, use pipes to display dates and currency values that are appropriate for a user's locale. Angular provides predefined pipes for common transformations, and you can also define your ownpipes. [18] .

2.12.5 Services and Dependency injection

For data or logic that isn't associated with a specific view, and developers want to share across components, they create a *service* class. A service class definition is immediately preceded by the @Injectable() decorator. The decorator provides the metadata that allows other providers tobe injected as dependencies into their class.

Dependency injection (DI) lets them keep their component classes lean and efficient. They don't fetch data from the server, validate user input, or log directly to the console; they delegate such tasks to services. [18]

2.12.6 Routing

The Angular Router NgModule provides a service that lets you define a navigation path among thedifferent application states and view hierarchies in your application. It is modeled on the familiar browser navigation conventions:

- Enter a URL in the address bar and the browser navigates to a corresponding page
- Click links on the page and the browser navigates to a new page
- Click the browser's back and forward buttons and the browser navigates backward andforward through the history of pages you've seen

The router maps URL-like paths to views instead of pages. When a user performs an action, such as clicking a link, that would load a new page in the browser, the router intercepts the browser's behavior, and shows or hides view hierarchies.

If the router determines that the current application state requires particular functionality, and the module that defines it hasn't been loaded, the router can *lazy-load* the module on demand.

The router interprets a link URL according to your application's view navigation rules and data state. You can navigate to new views when the user clicks a button or selects from a drop box, or in response to some other stimulus from any source. The router logs activity in the browser's history, so the back and forward buttons work as well.

To define navigation rules, you associate *navigation paths* with your components. A path uses a URL-like syntax that integrates your program data, in much the same way that template syntax integrates your views with your program data. You can then apply program logic to choose whichviews to show or to hide, in response to user input and your own access rules. [18].

The following diagram shows how these basic pieces are related.

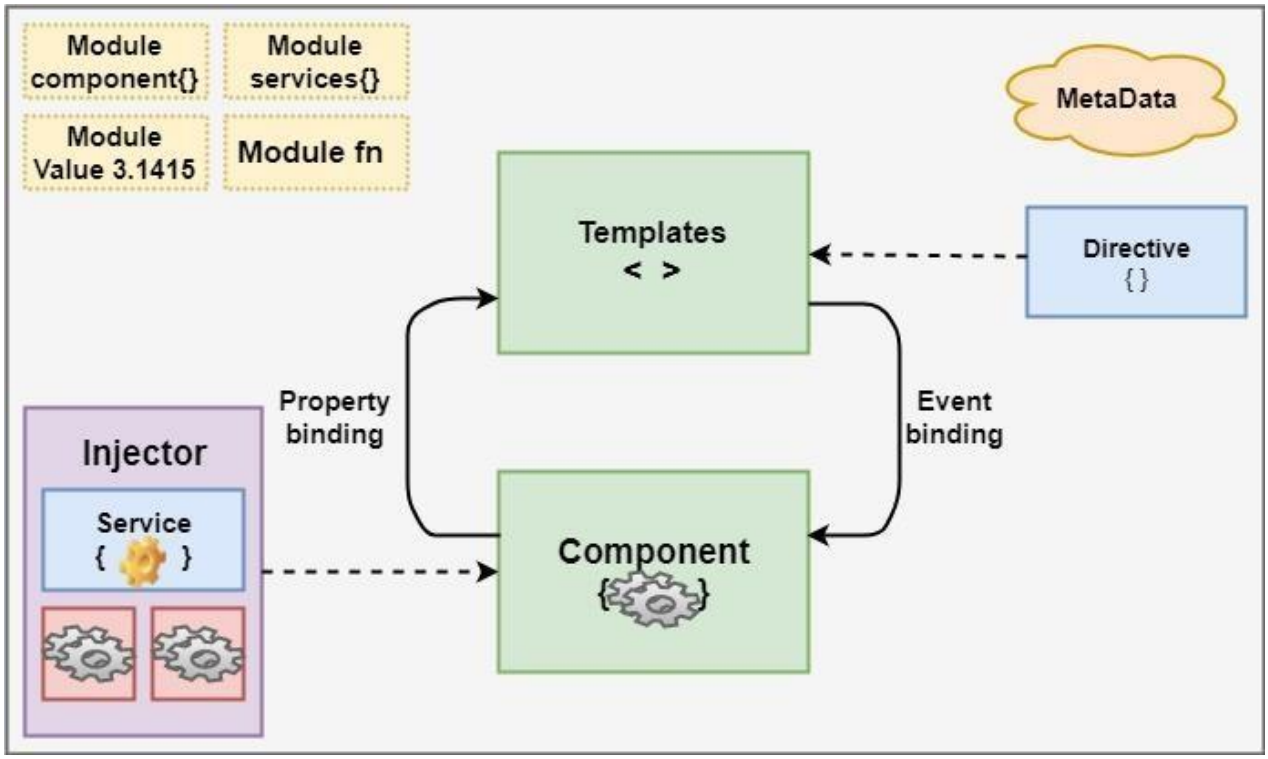


Figure 2. 8 : Angular Essentials

Chapter 3
Dashboard conception

3 Chapter 3: conception and system design

3.1 Introduction

this section is dedicated for fundamental development steps and ongoing process of the proposed ORM application, for the conception part, use case diagram, sequence diagram and workflow organigrams were selected to facilitate ,the understanding of each element part of the system. specification of needs:

the purpose here is to ensure the development of adequate and resilient software, compatible with the general description of the modeles maintained by banks, and this would be ,by answering the question: What are the functions of the system? so, system must meet the following requirements:

- should allow users the raise and create any sort of incident happening under the roof of the bank
- capture, collect, manage, track and report information about operational

loss events, key risk indicators, and risk and control assessments operational risk.

- facilitate Risk Assessment, cross module linkage, issues tracking and actions management, and management reporting.
- allow for analytical and management reporting that includes drilling down, adjusting, trend analysis, plotting operational

loss data at will, and scenario analysis. from dev perspective, system should be:

- Scalable and deployable across multiple entities and locations.
- Web-based
- user-friendly

3.2 risk assessment Formula

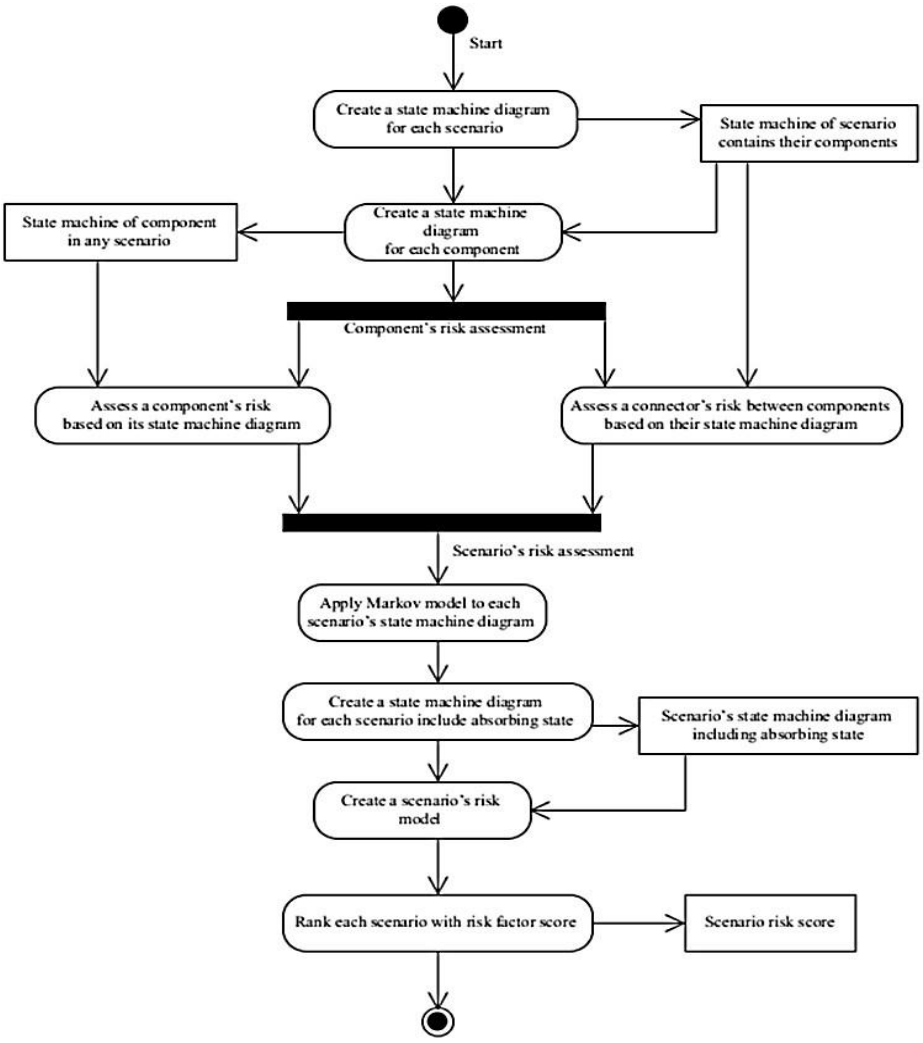


Figure 3. 1 : Activity diagram of the proposed risk assessment approach

The activity diagram is explained step by step as follows:

1. Create a state machine diagram for each component of each scenario. This step will generate a state machine diagram of components in scenarios effects the data in a relational database.
2. Risk Assessment consists of two steps:

2.1. Component risk assessment is calculated by using a model as shown here:

$$rf_i^x = PUOCS_i \ .\text{SVT}_i$$

rf_i^x: Risk factor of component i in scenario x

$PUOCS_i$: A probability of loss or injury of component i

SVT_i : Impact or severity of the undesired event of component i

2.1.1. Calculate the probability of a satisfactory component (PSC) transition from state p to q by using full predicate coverage criterion which will generate a number of test case as shown here:

$$\frac{|TrueTestCases_{pq}|}{|TotalTestCases_{pq}|}$$

$|TrueTestCases_{pq}|$: The number of test cases which make a correct transition from state p to q.

$|TotalTestCases_{pq}|$: The total number of test cases generated.

2.1.2. Calculate the probability of a satisfactory path through the state machine diagram using this formula:

$$PSC_{initial-final} = \prod_{i=0}^{n-1} PSC_{p_i p_{i+1}}$$

$PSC_{initial-final}$: A probability of a satisfactory path through the state machine diagram from the initial node to the destination node.

$PSC_{p_i p_{i+1}}$: A probability of a satisfactory transition between states. The result of this formula is the probability of state i multiplied by the probability of state (i+1).

2.1.3. Calculate the probability of an unsatisfactory path through the state machine diagram using this formula:

$$PUC_{initial-finale} = 1 - PSC_{initial-final}$$

2.1.4. Calculate the probability of an unsatisfactory outcome (PUOC) using this formula:

$$PUOC_i = \sum_{k=1}^{m} [\left[\frac{pp_k}{\sum_{l=1}^{m} pp_l}\right] . (PUC_{initial-finale})_k]$$

$PUOC_i$: A probability of unsatisfactory outcome of component i in each

scenario.

m: The number of possible paths in a state machine diagram.

K: The number of the path in state machine diagram.

pp_k: A product of the number of test cases in the k[th] path

$\sum_{l=1}^{m} pp_l$: A summary of the product of number of test cases in each possible path.

$(PUC_{initial-finale})_k$: The probability that the k[th] path will be unsatisfactory.

2.1.5. Normalize $PUOC_i$ to make it appropriate for the scenario x (S_x) by using this formula:

$$PUOCS_i = \frac{ppc_i}{\sum_{j=1}^{n} ppc_j} . PUOC_i$$

ppc_i : The total number of test cases generated for component i.

$\sum_{j=1}^{n} ppc_j$: The total number of test cases generated for every component in the same scenario.

2.1.6. Define the hazard score by using an entity relationship diagram. This score is calculated as shown in Fig below.

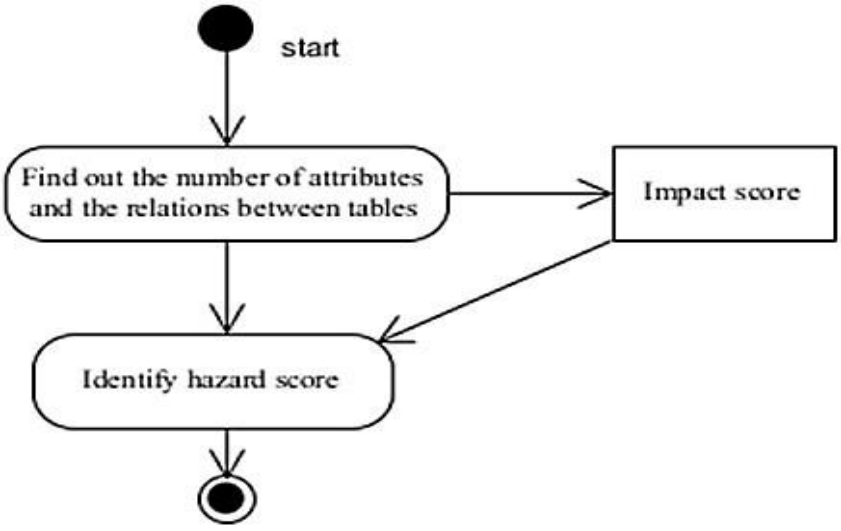


Figure 3. 2 : Activity diagram for identifying hazard score

2.2. Connector's risk assessment. Using the formula from Goseva-Popstojanova, each connector risk factor is calculated using the following formula.

$$EOC_{ij}^{x} = \frac{|MT_{ij}^{x}|_{i.j \in S_x, i \neq j}}{|MT^{x}|}$$

2.3. Scenario's risk assessment This step creates a scenario model based on state-based modeling. After the state machine diagram of each scenario is created, then the Markov property is applied on the state machine diagram in order to identify the probability of the transition one state to another.

2.3.1. Scenario's risk assessment. This model is represented by a control flow graph that contains a single start node and terminating node. The other nodes are used for representing an executable's software components. Those components are related to database schema-based constraints. Then a probability matrix is created by applying Markov property, so it means a probability of transition from component i to component j. This matrix is named as, P^x and its formula is shown here:

$$P_{ij}^{x} = \frac{n_{ij}^{x}}{\sum_j n_{ij}^{x}}$$

2.3.2. Create a software's scenario risk model Each transition of a scenario risk model is used to compute a probability in the transition probability matrix $\overline{P_{ij}^{x}}$. This matrix represents the case where a component i does not fail, and then the control is transferred to the component j, and finally the interaction between i and j does not fail. A formula for creating the transition probability matrix is shown here:

$$\overline{P_{ij}^{x}} = (1 - \mathrm{r}f_i^{x}).P_{ij}^{x}.\left(1 - \mathrm{r}f_{ij}^{x}\right)$$

After a software execution state machine diagram is created, it will be combined with abnormal execution states which imply hazard levels when software execution fails. A state machine contains (n+1) transient nodes where n is the number of components and a starting node, and (m+1) absorbing nodes where m is the number of failure nodes and a terminating node. Then a probability matrix is created by applying the Markov property on the state machine diagram.

This matrix is named as $\overline{P^{x}}$ and shown here:

$$\overline{P^{x}} = \begin{bmatrix} Q^{x} & C^{x} \\ 0 & 1 \end{bmatrix}$$

$\overline{P^x}$: The transition probability of all components in the scenario risk model.

Q^x: The (n+1) by (n+1) matrix of probability of transition from component to component

C^x: The (m+1) by (m+1) matrix of probability of transition from a component to failure node.

0: The (m+1) by (n+1) zero matrix.

1: The (m+1) by (m+1) identity matrix.

Each variable of the above formula is provided by the previous formulas. Therefore, it is possible to compute all probabilities of the transition matrix. Next, matrix A^x is defined to represent a probability that starting from a transient node will transition to an absorbing node. The formula used for generating matrix A^x is shown here:

$$A^x = (1 - Q^x)^{-1} C^x$$

Finally, the total probability of transition from a transient node to each kind of failure node is computed, and it is used to compute a risk factor score for the considering scenario.

2.4. Rank the scenario order by risk factor score This last step of risk assessment occurs when various scenario's risk factors in the software are calculated. A scenario risk factor score is ordered, so it will be easy to use in the risk management process.

3.3 General use case diagram

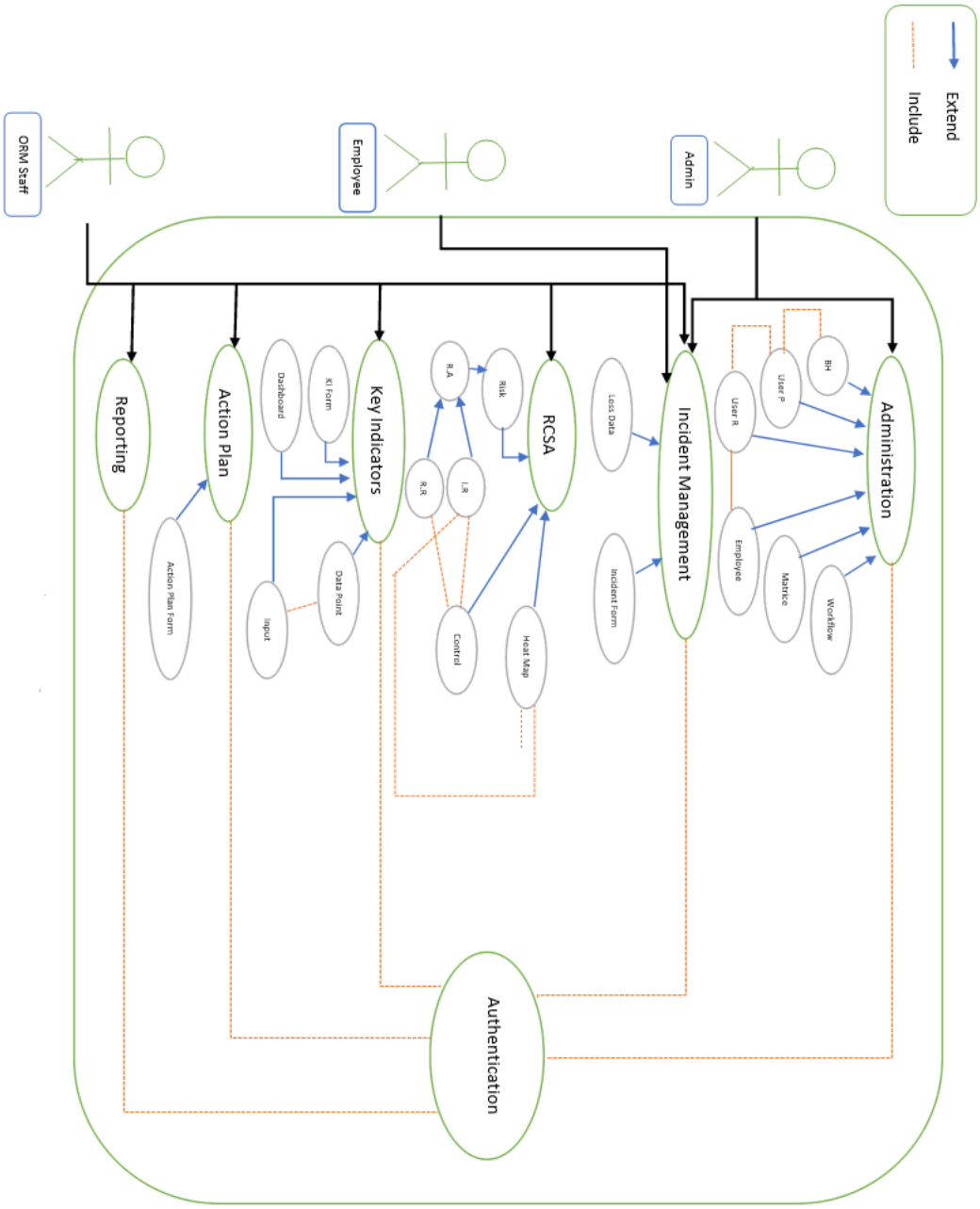


Figure 3. 3 : Use Case Diagram

3.4 Authentication sequence diagram

The following sequence diagram illustrates how the process is defined:

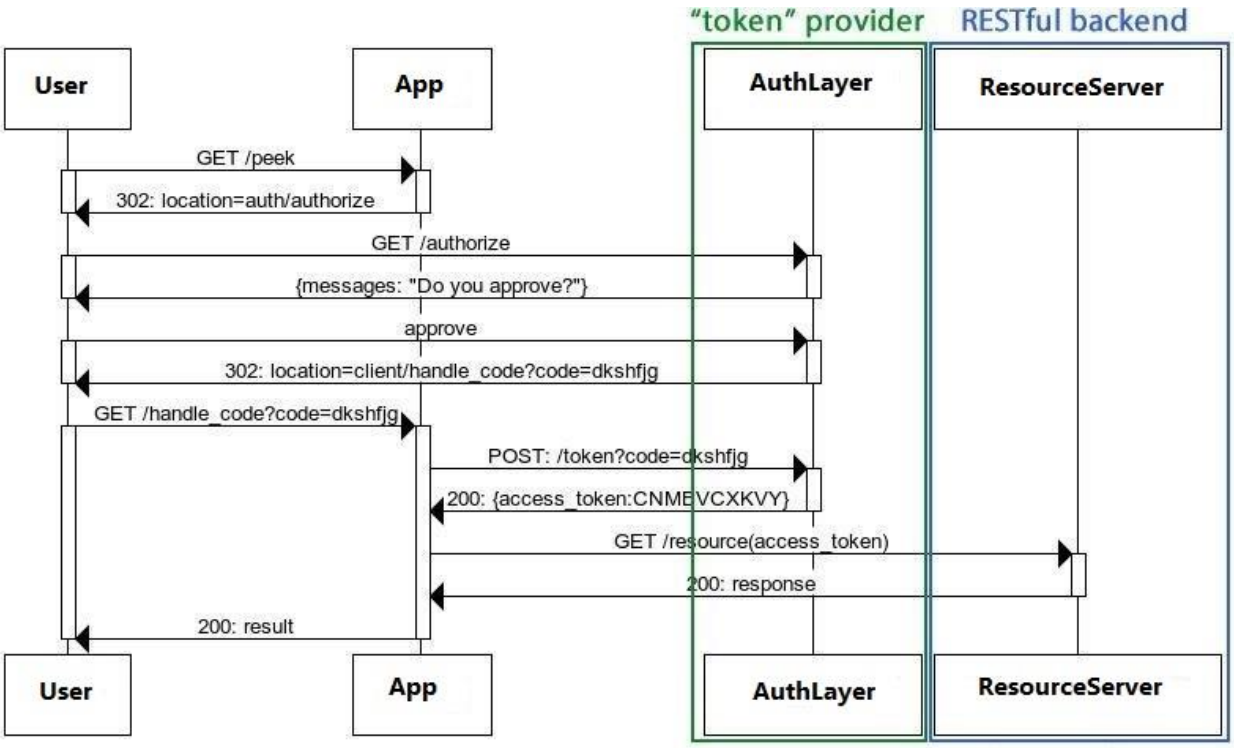


Figure 3. 4 : authentication sequence diagram

3.5 Risk identification and assessment database tables

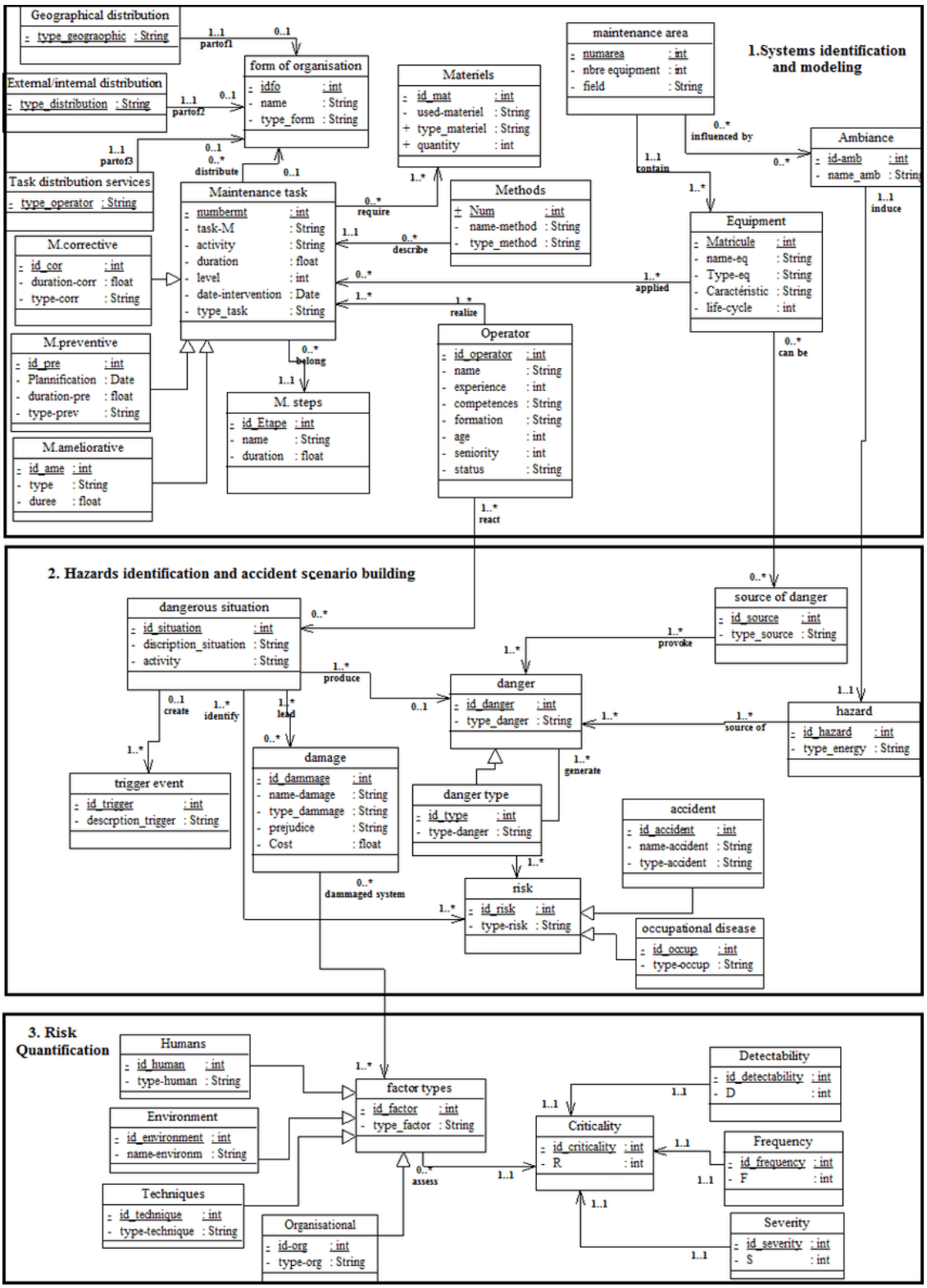
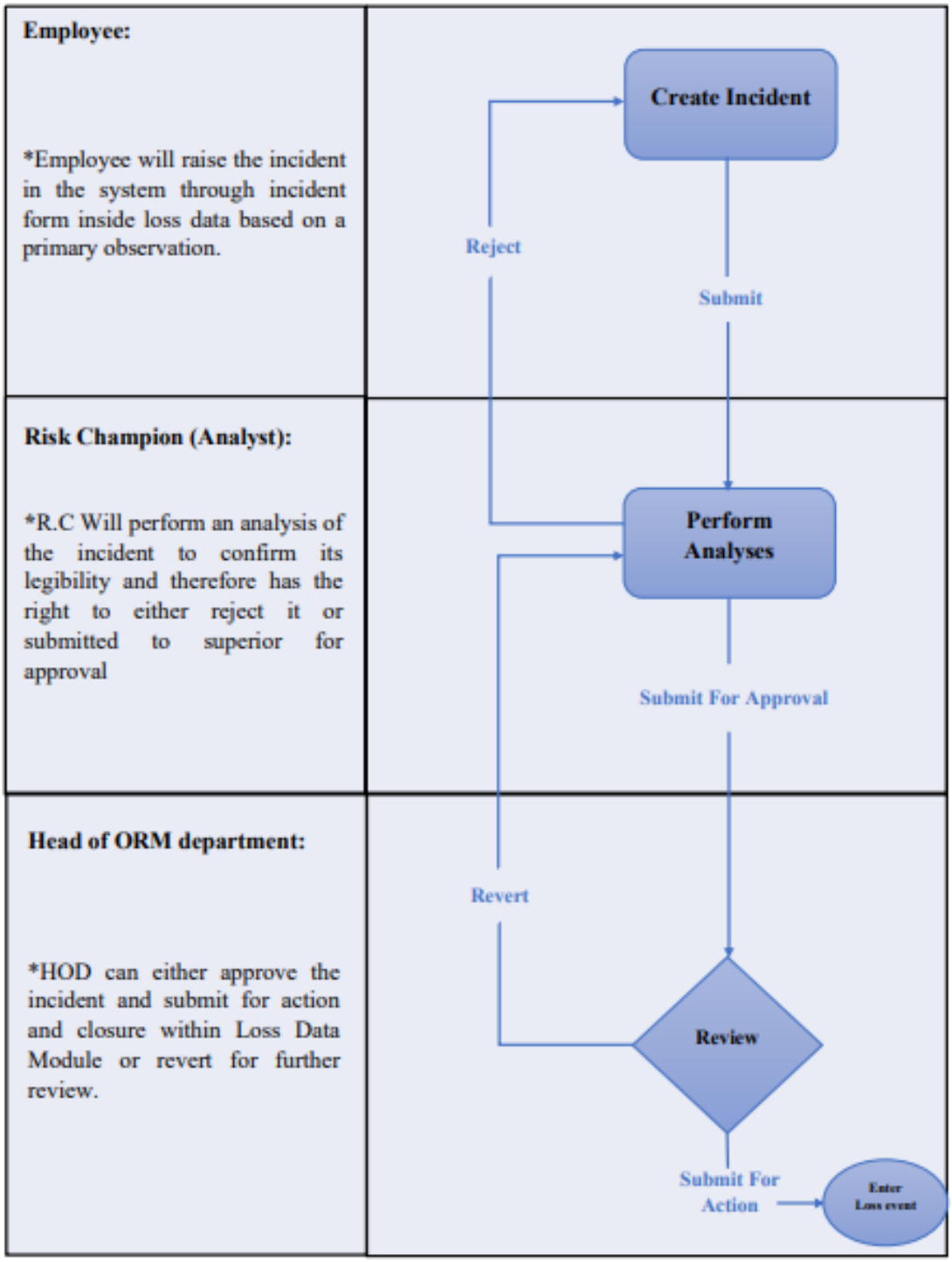
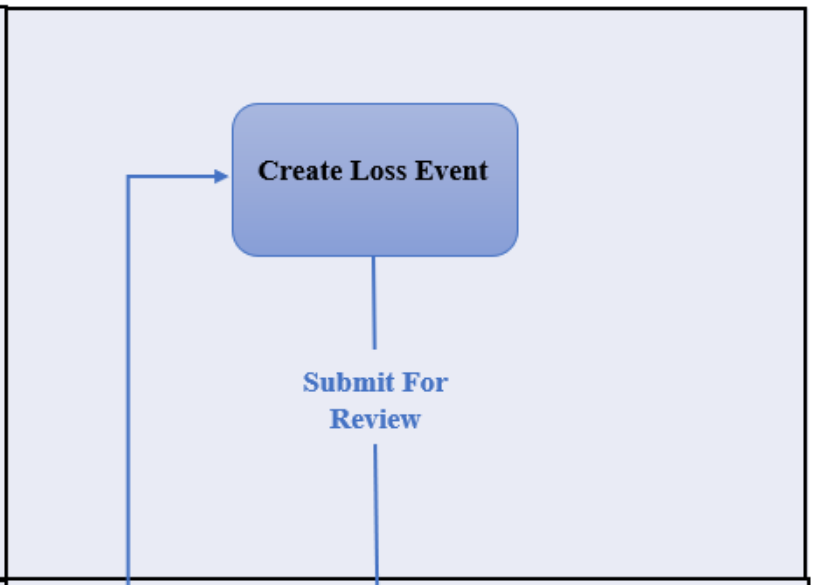
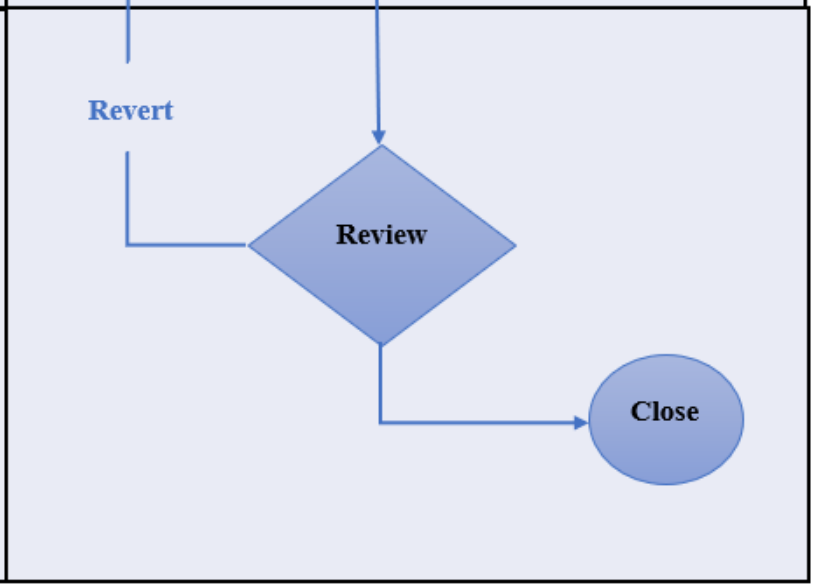


Figure 3. 5 : Database Tables

3.6 Incident Form Organigram



3.7 Loss data Organigram

Risk champion: *R.C will create the incident event that captures the actual loss accordingly with incident type, categorize it, defines its loss amount, attach existing evidence and link any possible action plan in addition to any related data and submit it to HoD for Review.	
HoD: *Hod will review if this last requires further investigation to revert it back or close it if the incident is fully covered.	

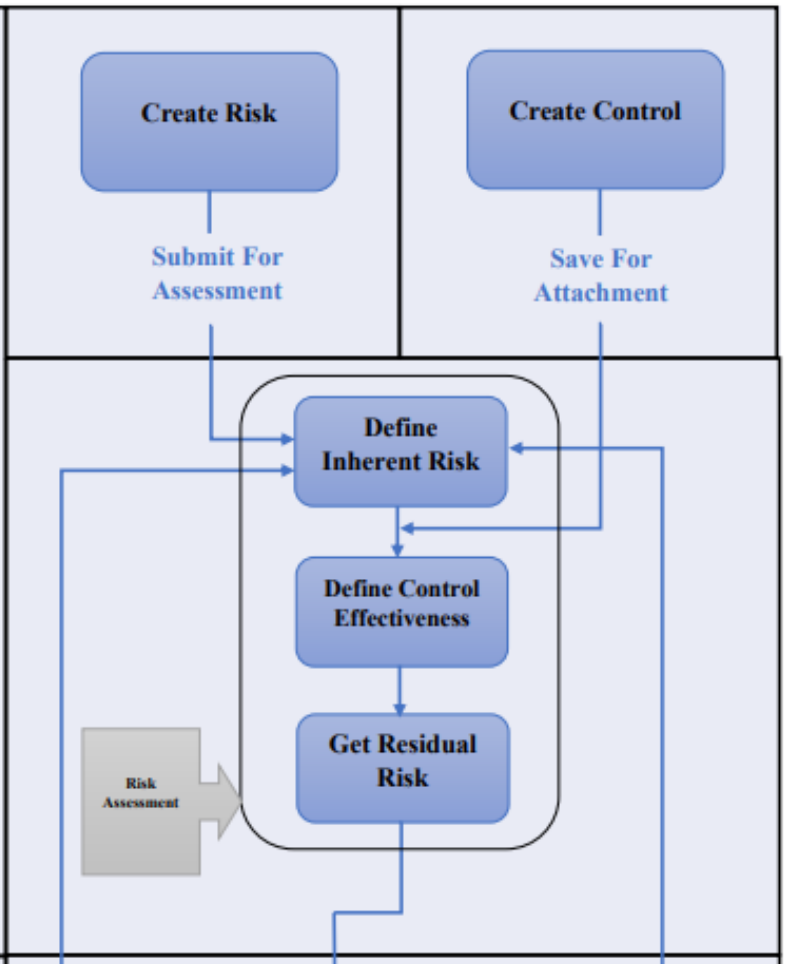
3.8 RCSA Organigram

Risk champion:

*R.C will create both risk and control, Risk Assessment get triggered after risk submission at R.C level which allows him to define the impact and likelihood the specific risk lays on to get a final inherent score.

*R.C will per next Attach a relative control and define its design and performance to get a final effectiveness score.

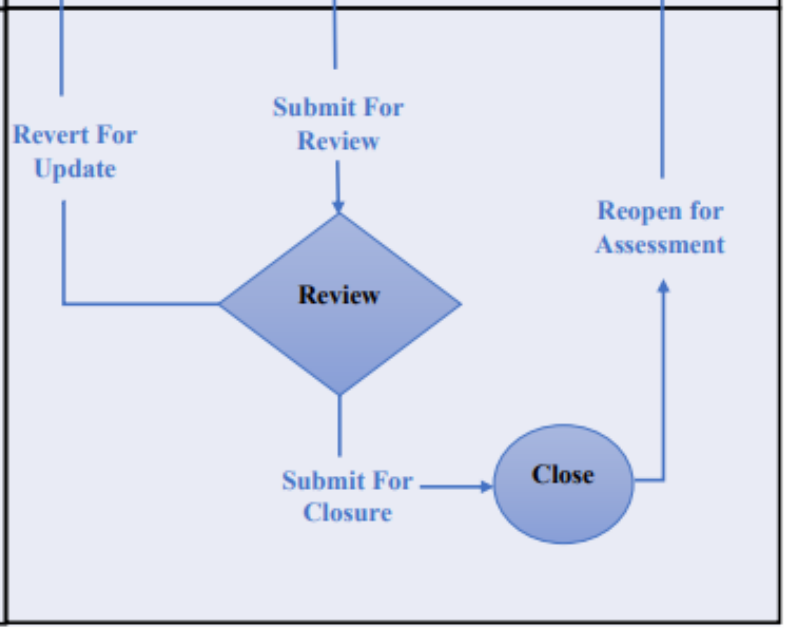
*Residual Risk Score will be auto generated based on previous scores according to a defined threshold (Low, Medium, High).



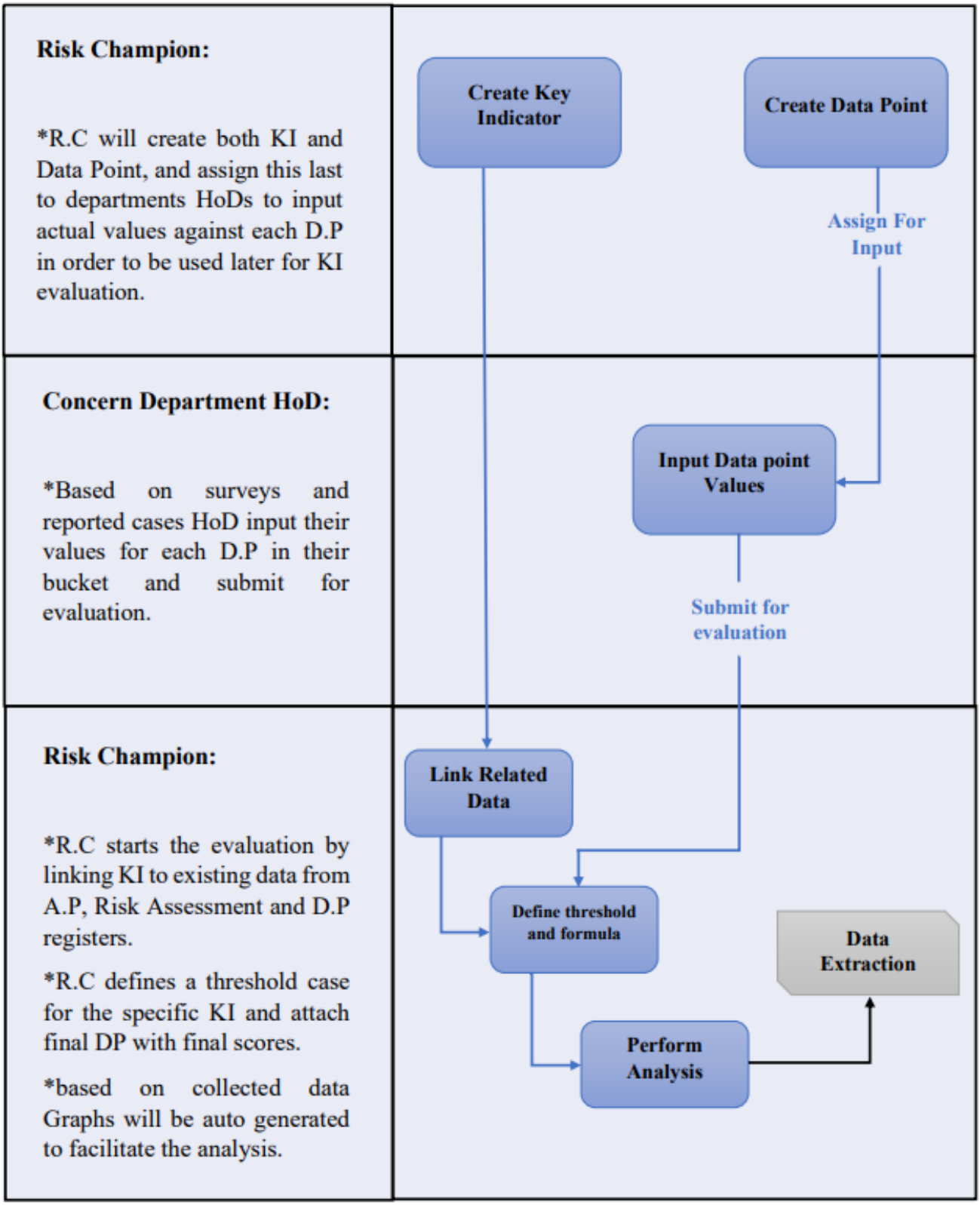
HoD:

*HoD gets a final result of the assessment for review where it can be reverted for improvement and update or submitted for closure

*Risk Assessment can be reopen for re-evaluation based on a defined frequency.



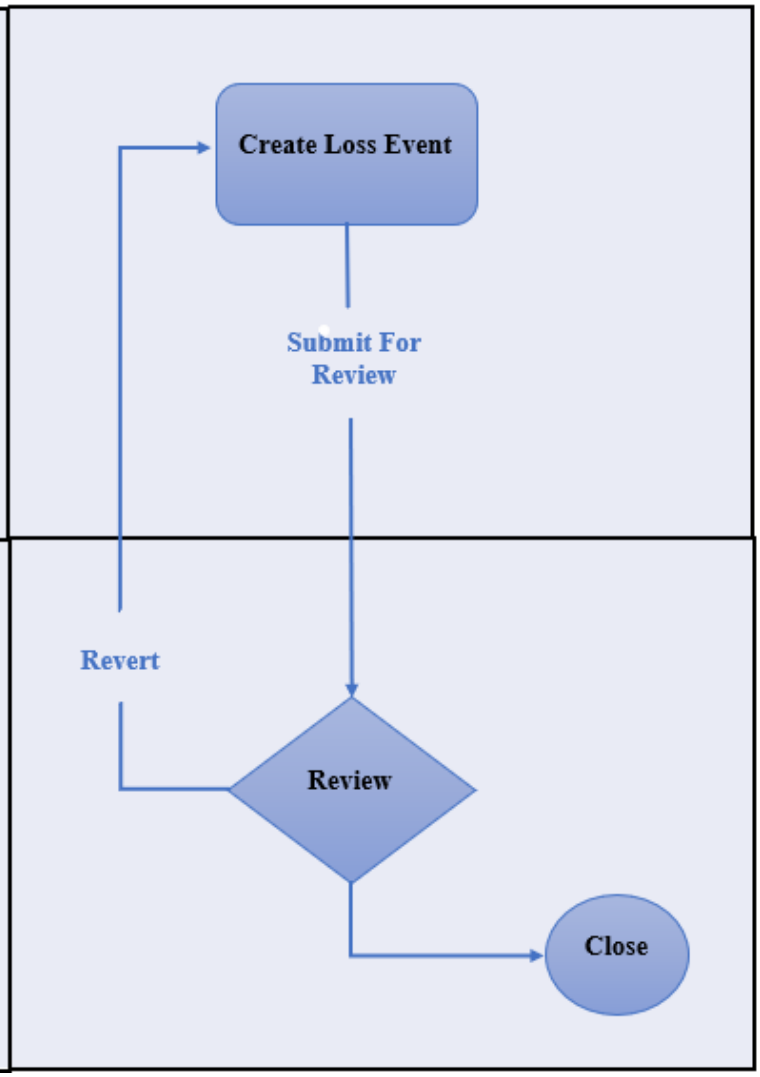
3.9 Key indicators Organigram



3.10 Action plan Organigram

Risk champion:

*R.C will create the Action Plan through form panel which defines measures to be taken against an incident that caused an actual loss.



Hod:

*Hod will look into the submitted action plan and its effectiveness, revert it back to R.C if an improvement is required or simply save and close it as an accepted A.P

Chapter 4
ORM system under oversigh

4 Chapter 4 : ORM system under oversight

4.1 General Application Features

This section outlines the common features in all modules of the ORM application

Standard Features

the application follows a user-friendly design schemeand feature offering. The following attributes are outlined in this section.

- **Application Login**
- **Cross-Module Access & Integration.**
- **Preference Setting**
- **Screen Optimization**

4.1.1 Application Login

To log in to the application, users can access the web link provided by IT administrators and signin using application login credentials. This App also offers Active Directory Domain Services (AD DS) and Single Sign-on (SSO) integration to simplify user management and enhancesecurity.

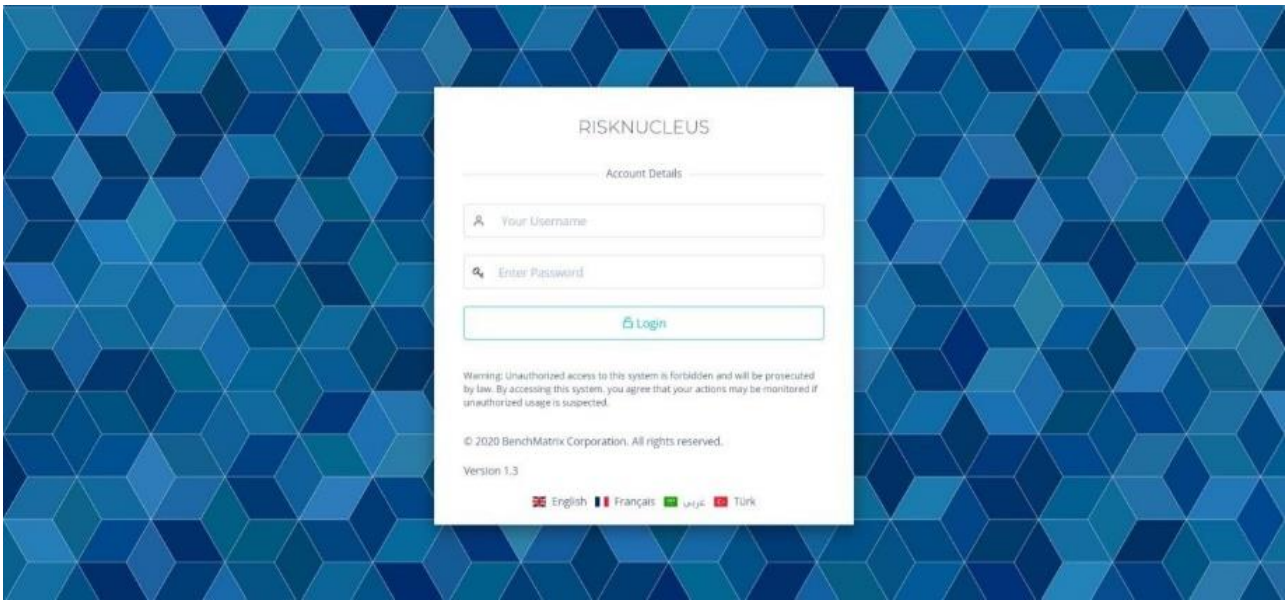


Figure 4. 1 : Application Login

4.1.2 Cross-Module Access & Integration

relevant data can be shared between synchronized modules and users with requisite privileges can access each application.

To access other modules within the Application,

1. Enter your **User ID** and **Password** on the **Login** page and click on the **Login** button
2. Once the system has verified your login credentials, click on your **Desired Module** from thelist appearing on the vertical navigation bar on the left hand side of the screen.

   Note: Only applications / modules to which you have access rights appear in the **Module Selection** modal

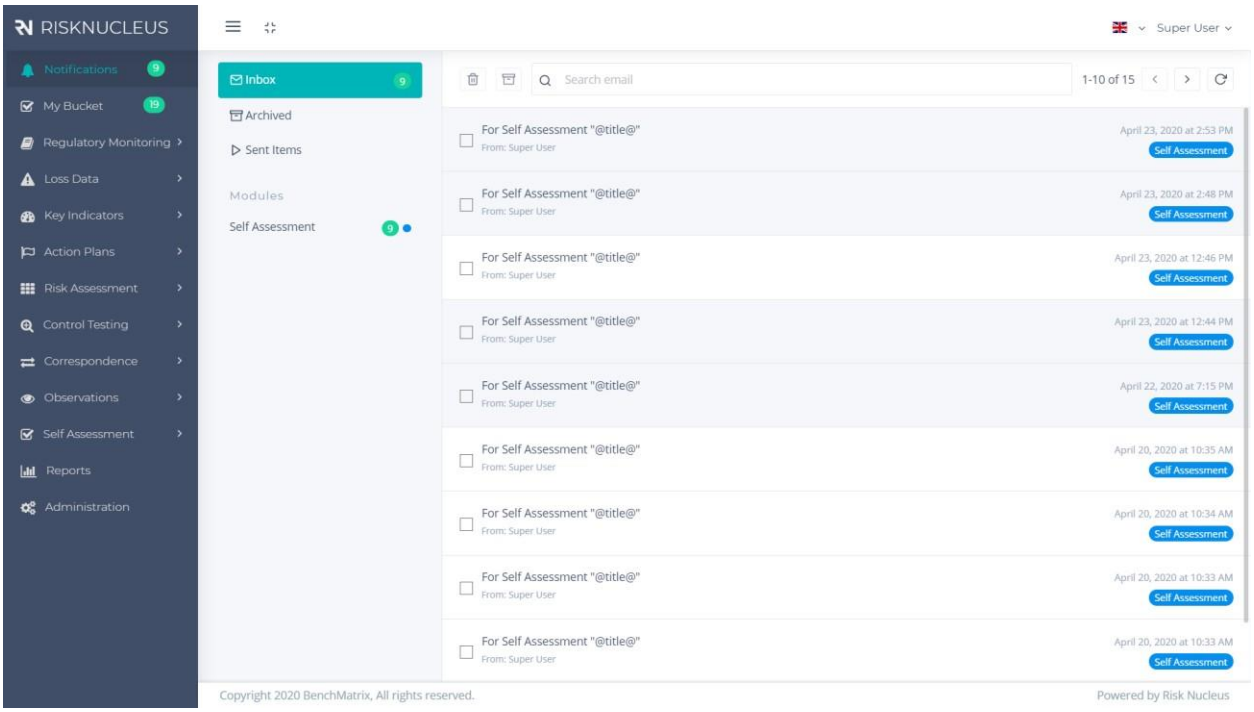


Figure 4. 2 : Module Selection

4.1.3 Navigation Bar

The **Navigation Bar** offers an easy way to navigate between key functionalities within the application. It is designed to enhance the user experience of the application. The Application offersa vertical menu with multiple drop downs. To navigate between pages:

1. Click on a label in the left hand side menu
2. Click on the respective label drop down to open the page

Note: Only pages to which you have access rights appear in the menu. Access rights can be configured through the **User Rights configuration** page.

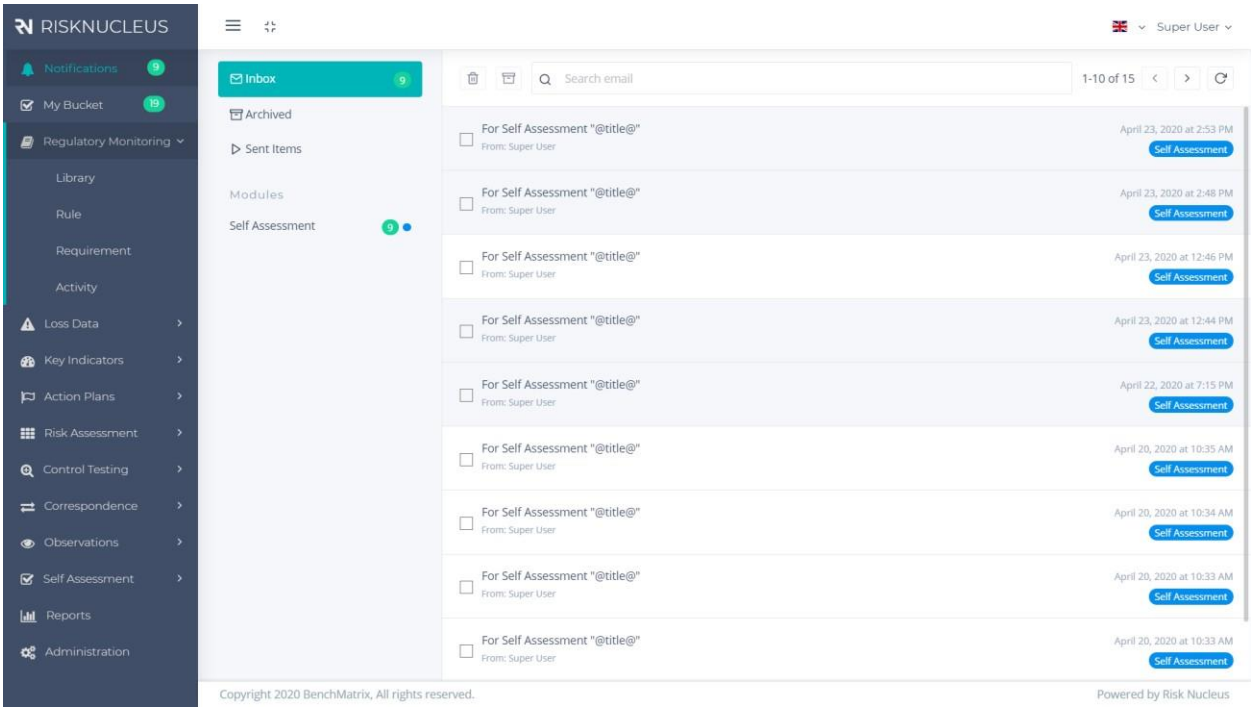


Figure 4. 3 : Navigation Bar

4.1.4 Listing Grids

The ORM Application employs standard grids to present itemized lists; for example, all communicationevents recorded appear in the correspondence module page in list form.

Listing grids offer standard features like Grid Search, Sorting, Filtering by Count and Pagination.To utilize these features, follow the steps below:

1. To perform a text search within records in a listing grid, enter your search term in the **Search** box above the top-right corner of the grid.
2. To sort items in ascending or descending order, simply click on the relevant column header.
3. To move between pages of records in the listing grid, click on the relevant **Page Number** orthe **Previous**, **Next**, **First** or **Last** buttons below the bottom-right corner of the grid
4. To show fewer or more records within a single page of the listing grid, select the *Number of Records* from the **Show *X* Entries** dropdown above the top-left corner of the grid

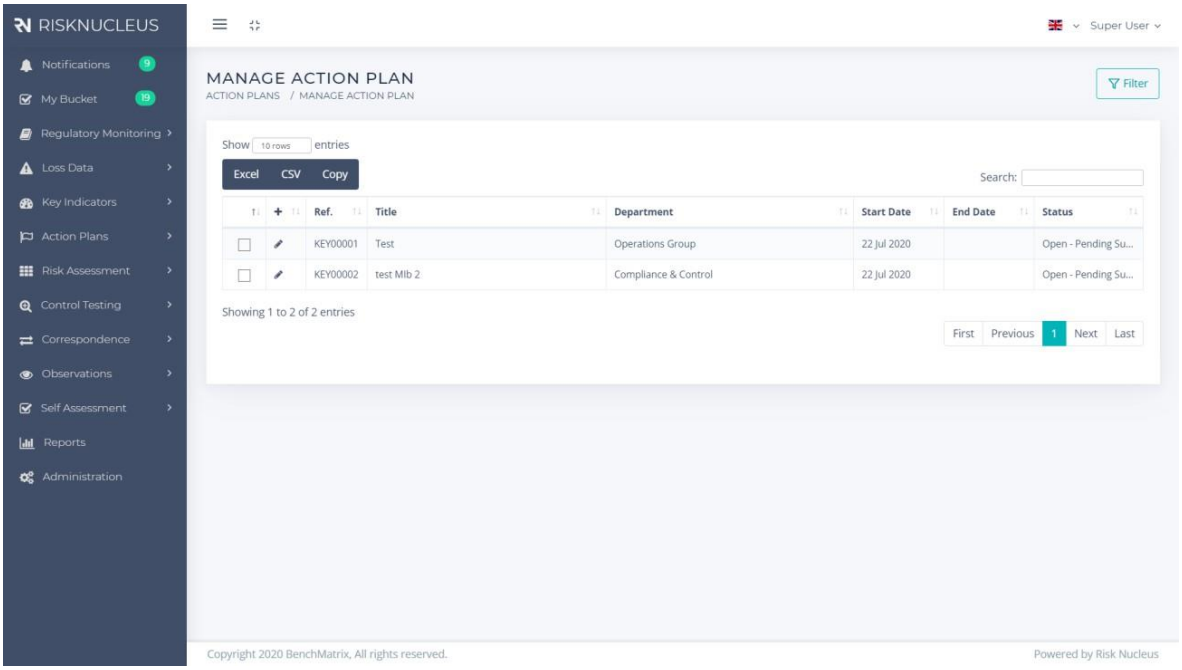


Figure 4. 4 : Listing Grid Features

4.1.5 Search Filters

In addition to the general grid search functionality, most listing pages offer Advanced Search filters to enable users to quickly navigate through a large volume of data. Search filters specific to each listing page are available near the top of the page.

To apply relevant search filters, follow the steps below:

1. Click on the **Filter** option to expand the function
2. Select relevant attributes in the filter fields available under filter; l
3. Click on the **Apply** button

To clear search filters applied, simply click on the **Remove** button in the Advanced Search accordion.

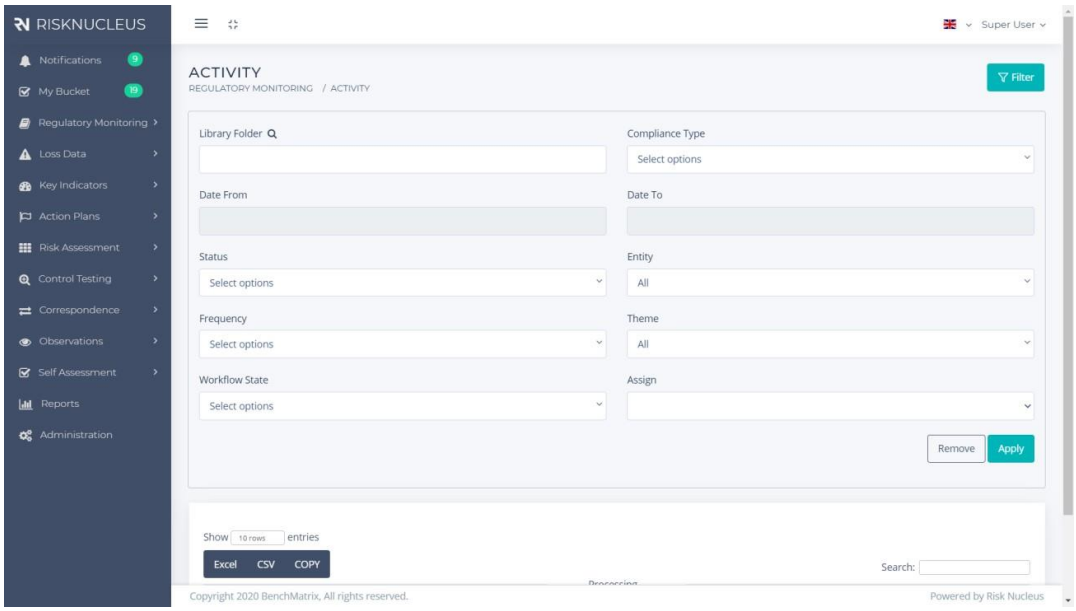


Figure 4. 5 : Search Filters

4.1.6 Audit Trail

A detailed track of all actions performed is maintained in the system to ensure system securityand data authenticity. Audit trails can be viewed by following the steps outlined below:

1. Go to the **Administration** page and click on the **System Audit** box
2. In the **Audit Trail** page, a full list of actions will appear on the main screen
3. Use the **search bar** for filtering the listing grid to show only records of interest; forexample, view actions taken on a specific page/module

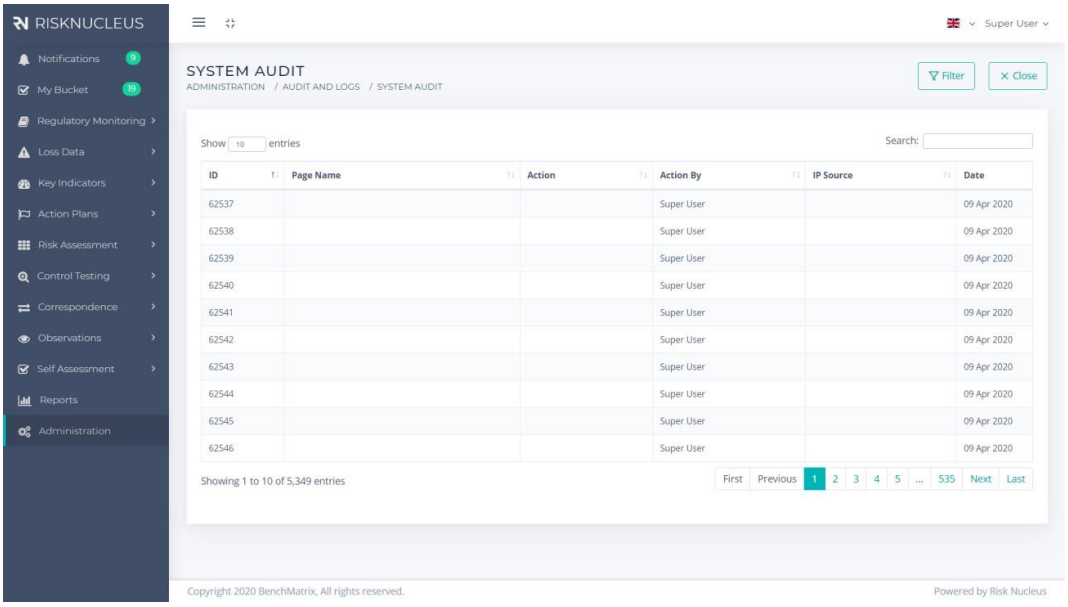


Figure 4. 6 : System Audit

4.1.7 Preference Setting

The ORM application allows the users to customize their respective screens according to their preferences. The functionality enables modification in areas of system language and defaultlanding page selection. Menu and workflow related options are also available to suit the needs ofa particular individual and enhance customer experience.

The **Preferences** screen can be viewed through following steps:

1. Enter your **User ID** and **Password** on the **Login** page and click on the **Login** button
2. On the top left corner of the screen, click on **User Profile** drop down
3. Select **Preferences** option

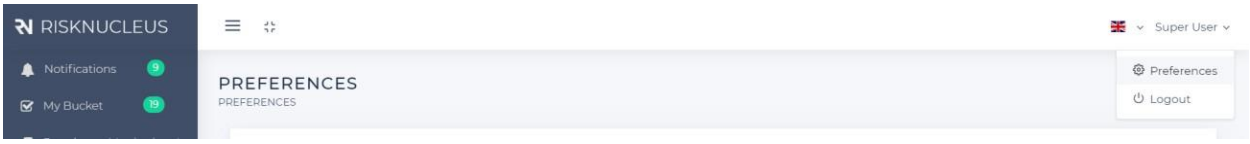


Figure 4. 7 : Preferences Option

A one pager screen will appear on clicking the preferences drop down option. Preference settingscan be customized on a user friendly interface. The options available on this screen include language settings and default homepage upon system login. Other options enable user to set preferences for workflow activity log view, menu view and changing the position of the menu. Once the required changes have been made, the **Update** button has to be pressed to enable thoseupdates on the screen.

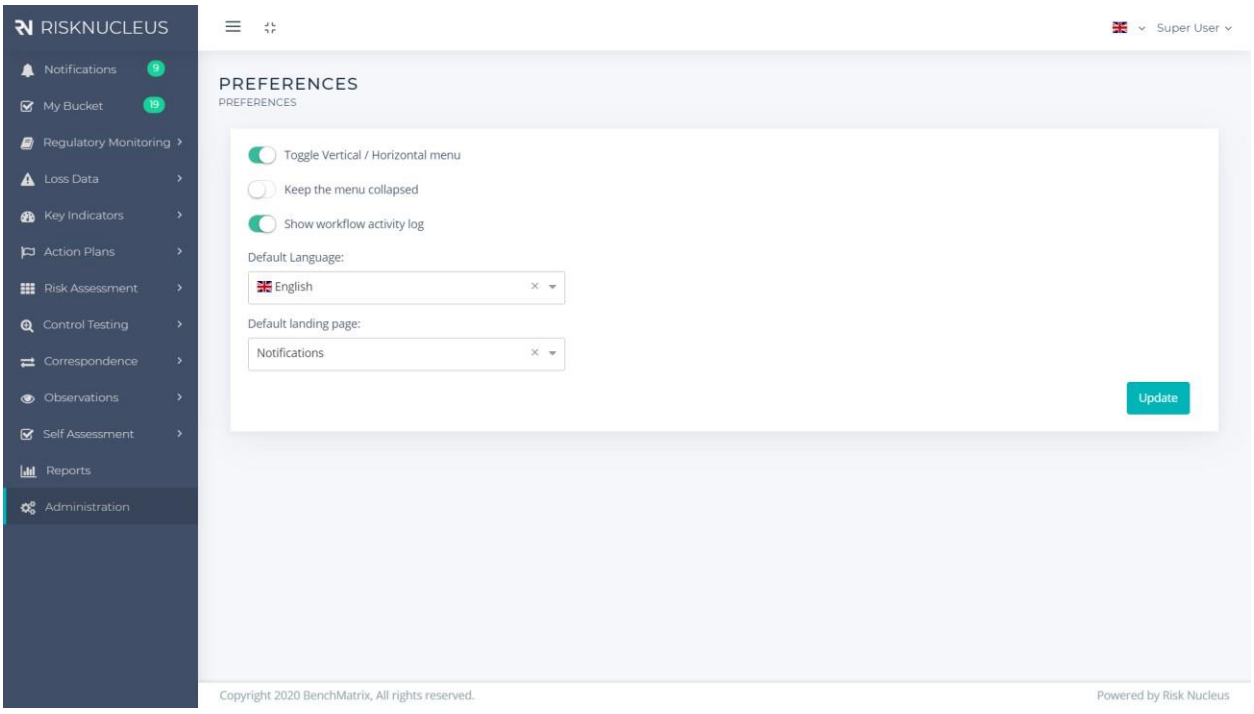


Figure 4. 8 : Preferences

4.1.8 Screen Optimization

The application interface has been designed keeping in mind user preferences and usage patterns.Design process is carried out after thorough deliberation, constructive feedback and ongoing trends. Following features are embedded to enhance this purpose:

4.1.8.1 Single process design

While using The Application , the user does not have to follow a series of steps or scroll certain number of pages to accomplish a task. The screen design allows selection mostly in one step and without opening additional windows.

For example, while creating a rule from the regulatory library, the rule addition page will nottrigger a separate window rather all actions can be performed on the same tab with **Close** option at the top to navigate easily across pages.

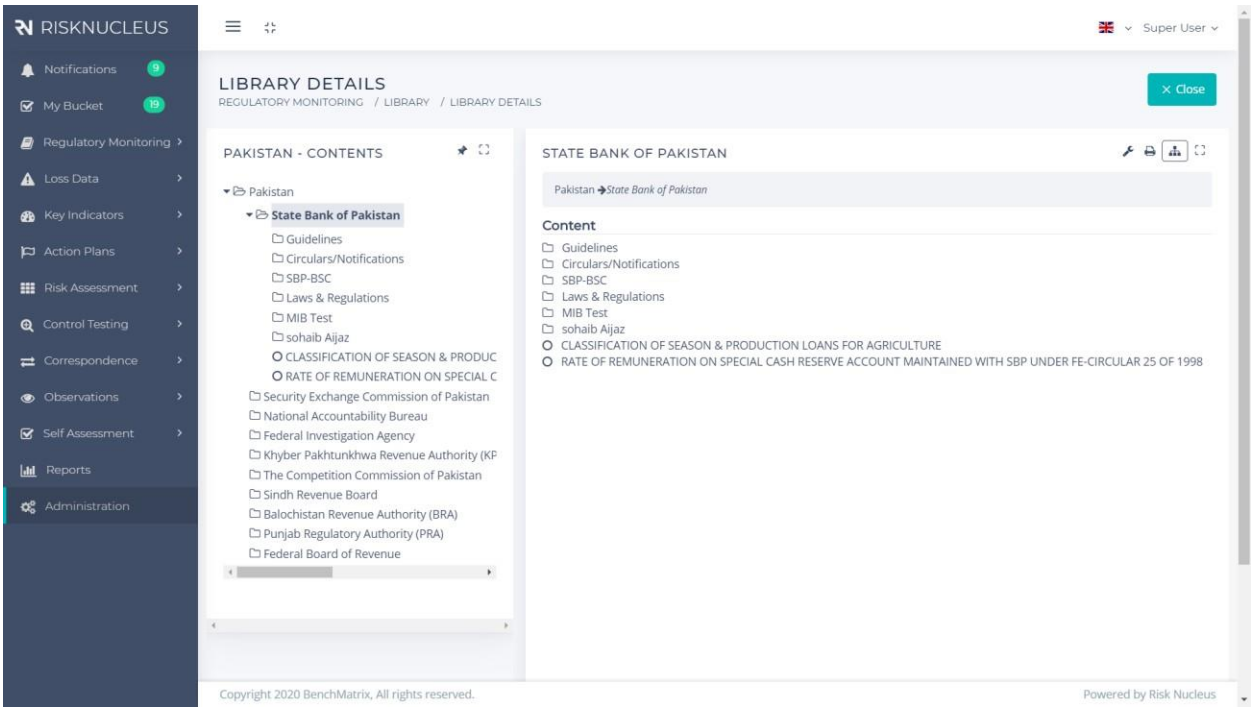


Figure 4. 9 : Single Process Design

4.1.9 Notification and My Bucket

Notification bar populates all the intimations regarding events being performed in the ORM application.

My Bucket refers to all activities pending to be performed by that particular user. Thissegregation facilitates in prioritizing critical tasks.

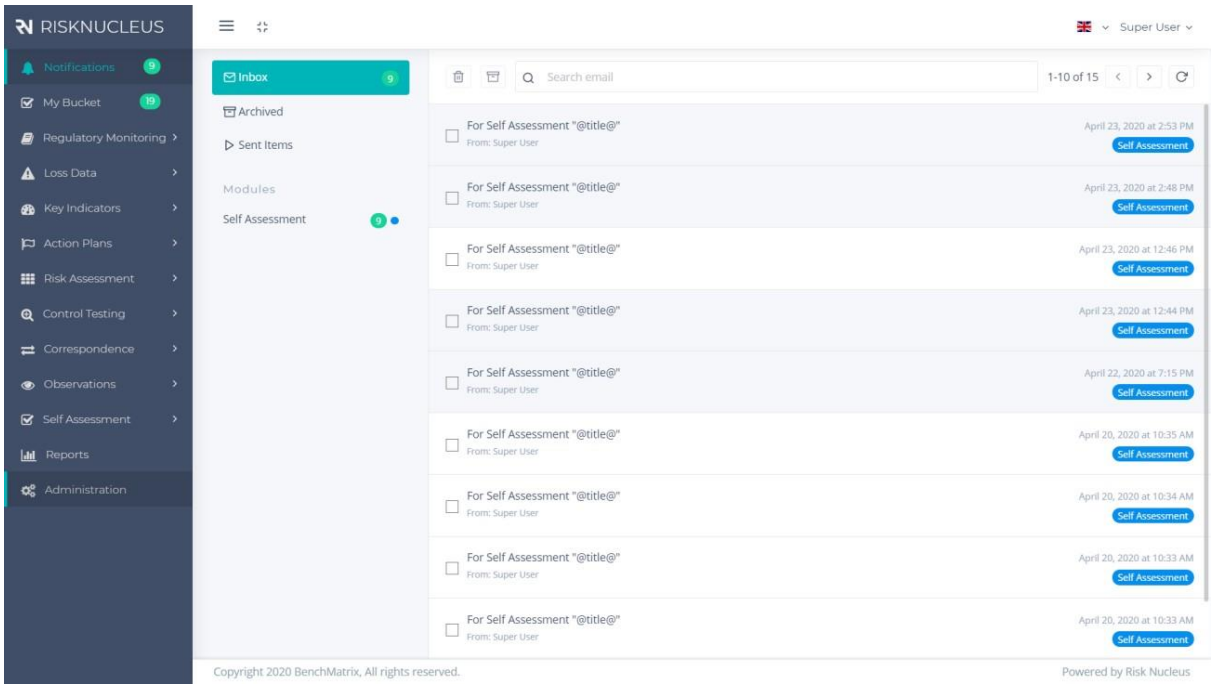


Figure 4. 10 : Notifications

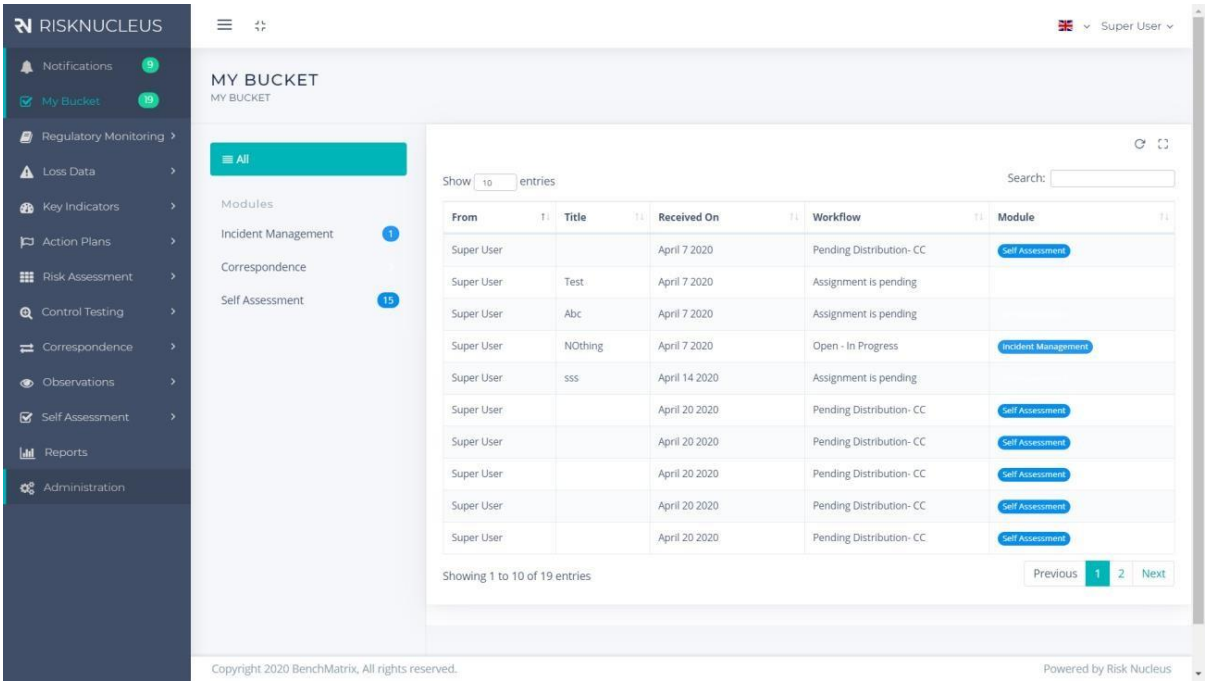


Figure 4. 11 : My Bucket

4.2 Administration

This chapter defines the high level configuration parameters and elements to be configured atthe time of application implementation along with more regularly configured elements like Organogram, user details, process workflows, risk measurement modeles, locations, user profiles/roles etc.

4.2.1 Introduction

Data and processes differ substantially between organizations. Within a single organization, multiple data points for a single entity may be maintained in a variety of different ways and requirements may change significantly over time.

4.2.2 Basic Information

This section outlines the process for accessing configuration pages and the basic process formodifying key configuration items.

4.2.3 Access Administration Page

To access the **Administration** page, use the following steps:

1. Enter your **User ID** and **Password** on the **Login** page and click on the **Login** button
2. Click on **Administration** option on the vertically aligned navigation bar

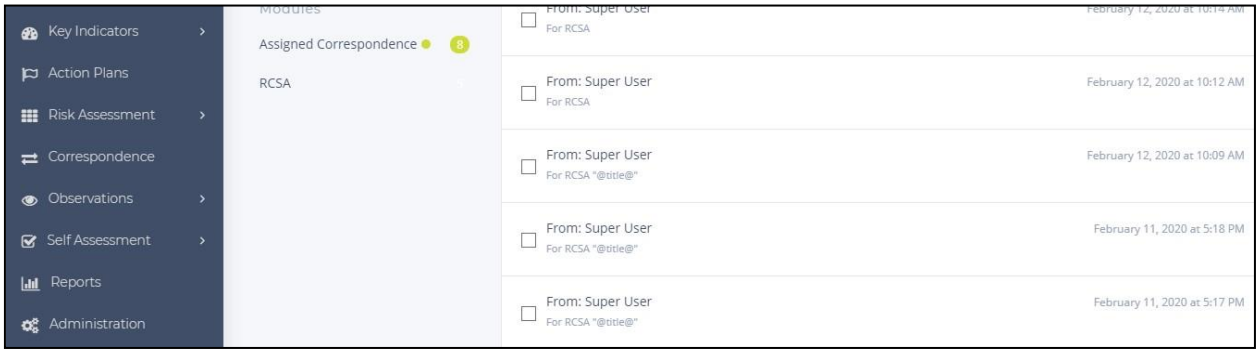


Figure 4. 12 : Access Administration Page

4.2.4 Access Category Page

To access category wise pages within the administration page, simply click on the relevant box containing the title of the item you wish to configure. Configuration pages are grouped togetherinto sections, shown as headings in the configuration page. Clicking on a configuration box willopen the relevant configuration page.

The sections under administration are as follows:

- ***General***

Tab	Functionality
Currency	Enables users to set default system currency.
Fields	Enables users to set various system fields
Emails & Notifications	Enables users to create & edit Emails & Notifications
Report	Enables users to create new system reports
Workflow State Type	Enables users to define the workflow states as required.
Menu	Enables users menu customization functionality
Prefix	Enables users to define system prefixes
Pages	Enables customization or changes in system pages.
Validation	Enables users to customize validation options and types.
Extract Report	Enables users to create and edit extracted reports.
Entity Replacement Setup	Provides the functionality to replace system entities as required.
Library Update	Provides manual upload functionality for library update, along with template.
Language	Enables users to select default system language.
Field Link Pages	Provides functionality for field linkages of pages.
Workflow Setup	Provides workflow setup functionality
Module	Provides system module customization
Employee Replacement Setup	Provides the functionality to replace employees within the system when required.
Data Uploader	Bulk data uploader functionality for different system configurations.

- ***Model & Hierarchy***

Tab	Functionality
Levels	Enables definition of system entity levels
Business Hierarchy	Enables creation & setting of system hierarchy
Product	Enables definition of user products as appropriate
Business lines	Enables definition of business lines as required.
Process	Enables process definitions and creations
Locations	Enables definition of geographical locations
Office type	Enables definition of office type

- ***Users***

Tab	Functionality
Employee Replacement	Enables replacement of employees within the system as required.
Employee	Enables manual employee creation.
Entity Replacement	Enables replacement of entity as required.
Designation	Enables designation definition as appropriate.
User Profiles	Enables creation and user profile rights definition.
Employee Status	Enables employee status changes as required.

- ***Regulatory Correspondences***

Tab	Functionality
Source	Enables definition of different correspondence sources.
Channel	Enables definitions of various channels for correspondence receiving.
Correspondence Nature	Enables definition of different types of correspondences.

- ***Compliance***

Tab	Functionality
Industry Library	Enables viewing of the compliance industry library.
Schedule Service	Enables single button service of different compliance related system functionalities.
Broad Category	Enables definitions of compliance broad categories.
Rule Status	Enables definitions of different rule statuses.
Resolution Type	Enables definitions of different types of resolutions.
Activity Priority	Enables definition of activity priorities.

Regulation Type	Enables definitions of different types of regulations
Requirement Status	Enables definitions of different requirement statuses.
Compliance Type	Enables the definition of type of compliance.

- ***Audit & Logs***

Tab	Functionality
Sent Mail Log	Sent mails log within listing grid.
Failed Mail Log	Failed mails log within listing grid.
System Audit	Record of system audits within a listing grid.
Successful Audits	Record of successful audits in a listing grid.
Manual Reminder	Record of manual reminders in a listing grid
Failed Audits	Record of failed audits in a listing grid

- ***Questionnaire***

Tab	Functionality
Questionnaire Answer Type	Enables definition of different types of answers for questionnaires.
Certification Type	Enables certification types for different questionnaires.
Category Assessment	Enables definition of different assessment categories.
Tag	Enables definition of tags such as IRAF or ELC for questionnaires.

- ***Categorization***

Tab	Functionality
Risk Categories	Enables definition of risk categories.
Event Type	Enables definition of event type categories.
Causal Categories	Enables definition of causal categories.
Impact Categories	Enables definition of impact categories.
GL Accounts	Enables definition of GL account categories.
External Causal	Enables definition of External Causal categories.
Individual Involved	Enables definition of individuals involved.
Loss Control Status	Enables definition of loss control statuses.
Incident Type	Enables definition of incident types.
Potential Customer Impact	Enables definition of potential customer impact categories.
Potential Loss	Enables definition of potential loss categories.
Product Link Process	Enables definition of product link processes.

Recovery Type	Enables definition of recovery types.
System Name	Enables definition of system names.

- ***RCSA***

Tab	Functionality
Assessment Type	Enables definition of assessment types.
Assessment Category	Enables definition of assessment categories.
Assessment Dimension	Enables definition of assessment dimensions.
Assessment Dimension & Area	Enables definition of assessment dimensions and areas.
Assessment Measure	Enables definition of assessment measures.
Assessment Measure Values	Enables definition of the values used in assessment measurement.
Assessment Measure Weightage	Enables definition of weightages in assessment measurement.
Score Threshold	Enables definition of score thresholds.
Risk Type	Enables definition of risk types.
Formula	Enables definition of formulas for RCSA.

Risk & Control Assessment Definition	Enables new RAM creation as appropriate.

- ***KI***

Tab	Functionality
KI Dashboard	Enables creation of new KI dashboards as required.
KI Direction	Enables definition of KI directions.
KI Type	Enables definition of KI types.
KI Type Categories	Enables definition of KI type categories for classification.
KI Thresholds	Enables definition of KI thresholds.
KI Impact Type	Enables definition of KI impact types.
KI Format	Enables definition of KI formats.
KI Threshold Category	Enables definition of KI threshold categories for classification.

- ***Action Plan***

Tab	Functionality
Action Plan Type	Enables definition of type of action plans.
Action Plan Severity	Enables definitions severity for action plans.
Action Plan Category	Enables definition of categories for action plans.

- ***Control Plan***

Tab	Functionality
Control Plan Threshold Category	Enables definition of threshold categories for control plans.
Control Plan Status	Enables definitions of control plan status type.

4.2.5 Workflows and Statuses

As is standard in the application, each key item can be processed through a configurable workflow that can serve both as a standard business workflow and also as a reviewcycle. Workflow steps can trigger changes in the item's Activity Status, the overarching status associated with an item and typically used in reporting.

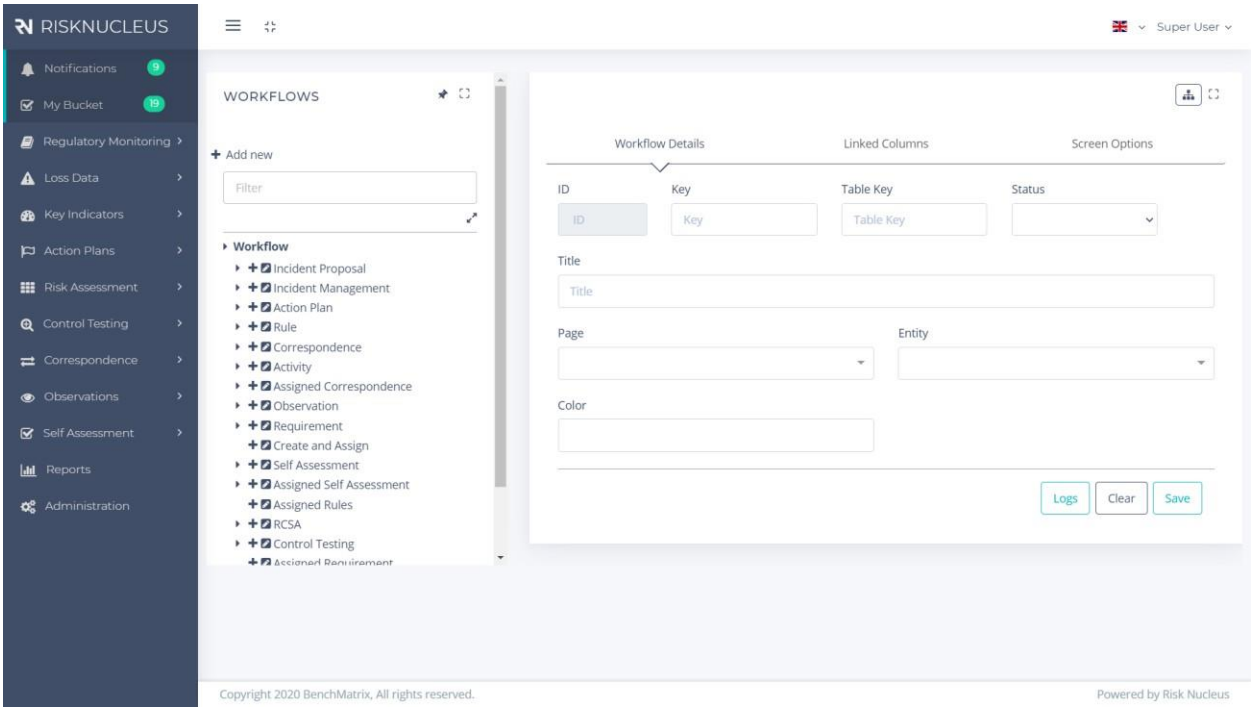


Figure 4. 13 : Workflow Setup

4.3 Loss Data

This chapter outlines the key functionalities of the Loss Data module of the application. Thecontents are divided into following sections:

- ***Introduction***
- ***Incident Proposals***
- ***Detailed Incidents***

4.3.1 Introduction

Loss data recognition and realization is an integral part of managing operational risk. The traditional attitude towards operational risk overlooked the importance of recording and automating the process of recognition and realization of loss data spawning from different departments during their operations.

The application Loss Data module provides the functionality to input all Loss Data generated and formulate action plans accordingly for future prevention. This is done in the form of incident proposals that aim to capture each potential loss generating incident and prevent repetition through adequate action plans and the reflection of the same on the operational risk management process of the organization.

4.3.2 Incident Proposals

Incident Proposals functionality is provided to capture each potential loss / breach makingincident in the system and linking with appropriate action plans.

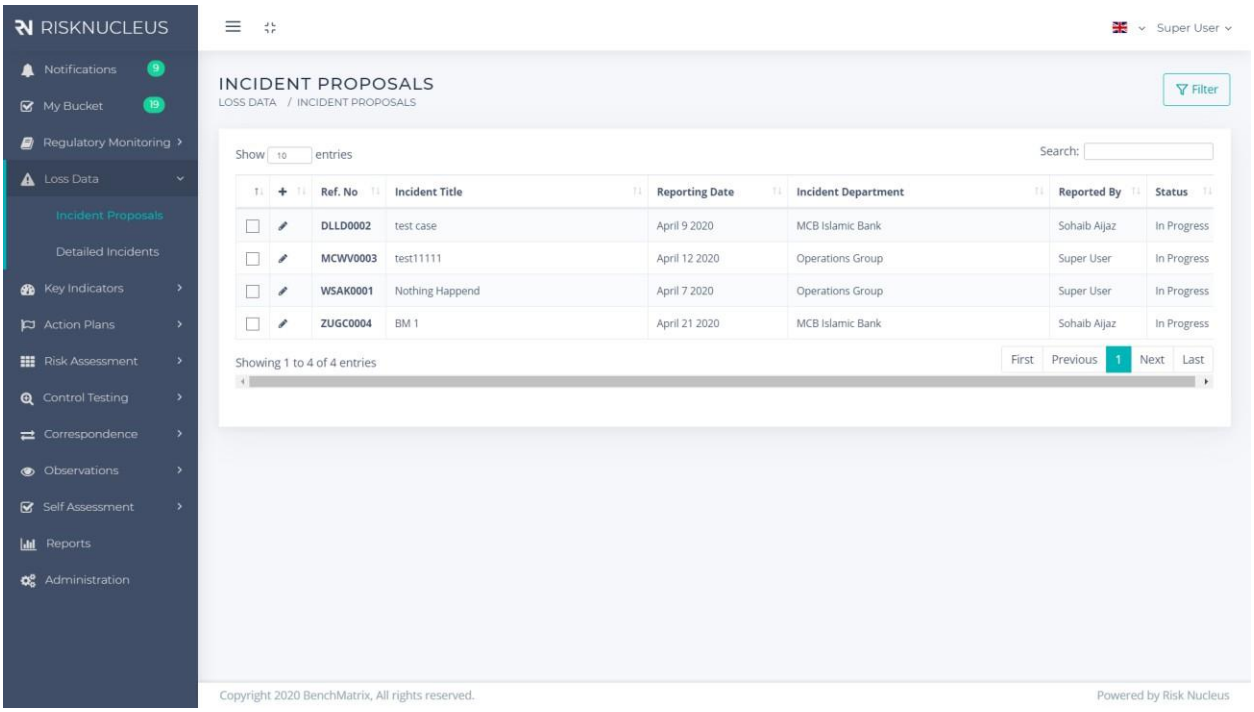


Figure 4. 14 : Incident Proposals

4.3.3 Adding Incident Proposals

The application Loss Data module gives the user the option to record new incident proposals orbreach when required for appropriate incident management.

To add a new Incident Proposal, follow the steps below:

1. On the navigation bar, click on the **Loss Data** label to open the drop down list
2. Select and Click the **Incident Proposal** option to open the window
3. Press the "+" button on the header row of the listing grid
4. Incident Proposal window opens.

Note: Only pages to which you have access rights appear in the menu. Access rights can be configured through the **User Rights configuration** page.

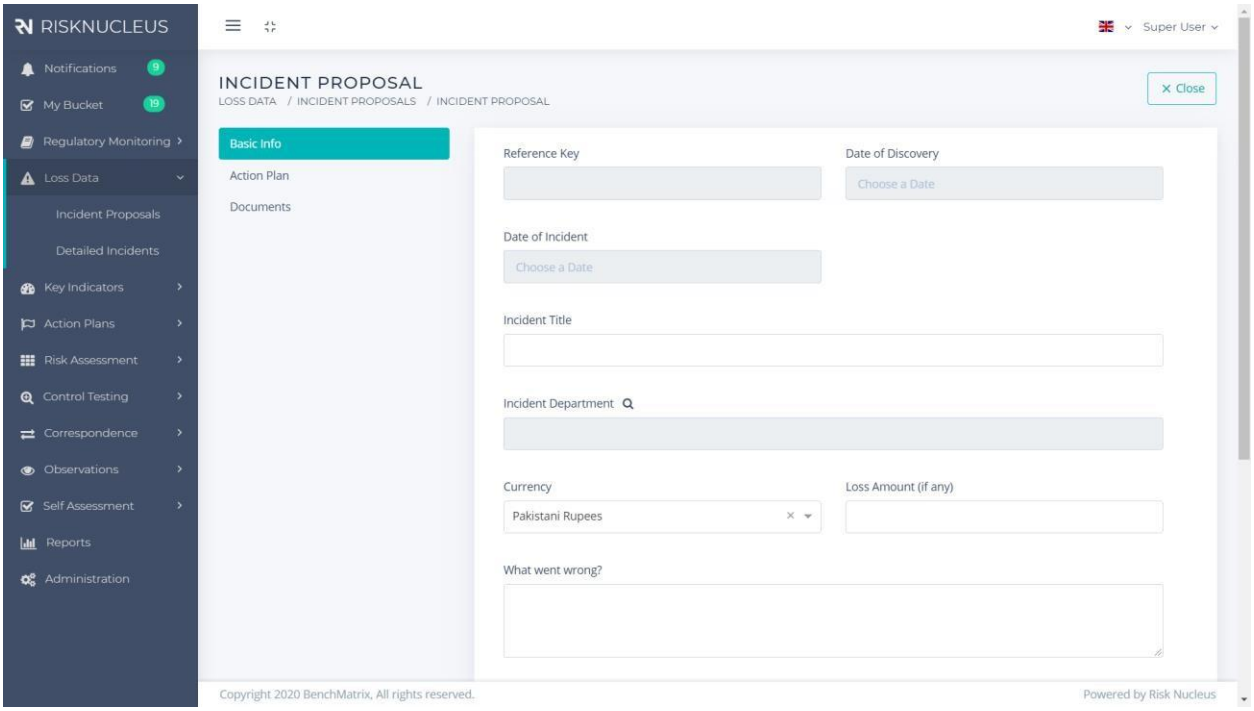


Figure 4. 15 : New Incident Proposal

Following fields are required to be filled when adding a new incident proposal

Attribute	Description
Reference Key	Unique attributes assigned by the system automatically for differentiation
Date of Discovery	Refers to the date the incident was discovered.
Date of Incident	Refers to the date the incident originally occurred.
Incident Title	Incident name or description.
Currency	Currency in which the loss occurred if any.
Loss Amount (If Any)	Reflects the amount of loss incurred if any in the currency thatis selected.
What Went Wrong	Description of what enabled the incident to occur.
How Was it Discovered	Description of how the incident was discovered after occurrence.
Action Taken (If Any)	Details of the actions taken after the incident had occurred.

Other Tabs

Tab Name	Functionality & Purpose
Action Plan	Enables the linkage of incident with an appropriate action plan as required.
Documents	Supporting documents or the original documentary evidence relating toa requirement as received from the regulator can be uploaded here.

4.3.4 Detailed Incidents

The detailed incident functionality is provided to capture incidents that require enhanced investigation and reporting that reflects the nature of the incident. Similar to the incident proposals, detailed incidents can be used at the discretion of the user when deemed necessaryaccording to the incident in question.

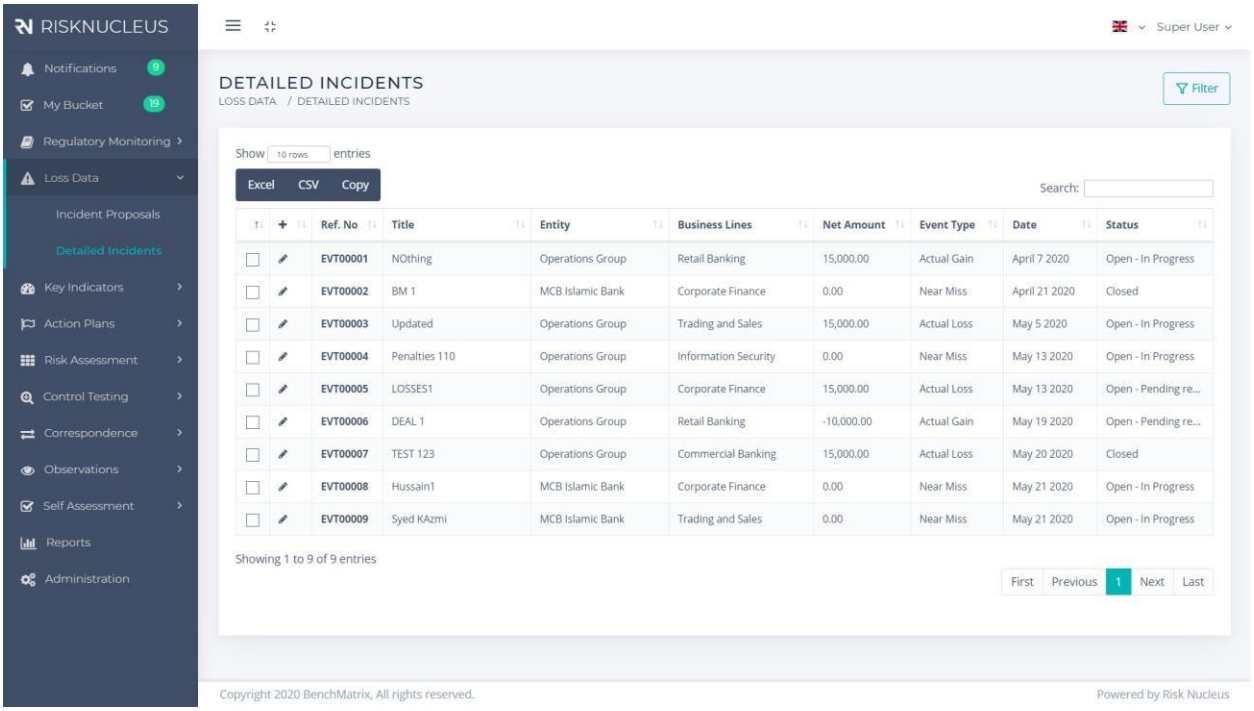


Figure 4. 16 : Detailed Incidents

4.3.5 Adding Detailed Incidents

The application Loss Data module offers the functionality to add detailed incidents as required based on users needs.

To add a new Detailed Incident, follow the steps below:

1. On the navigation bar, click on the **Loss Data** label to open the drop down list
2. Select and Click the **Detailed Incidents** option to open the window
3. Press the "+" button on the header row of the listing grid
4. New Detailed Incident window opens.

Note: Only pages to which you have access rights appear in the menu. Access rights can be configured through the **User Rights configuration** page.

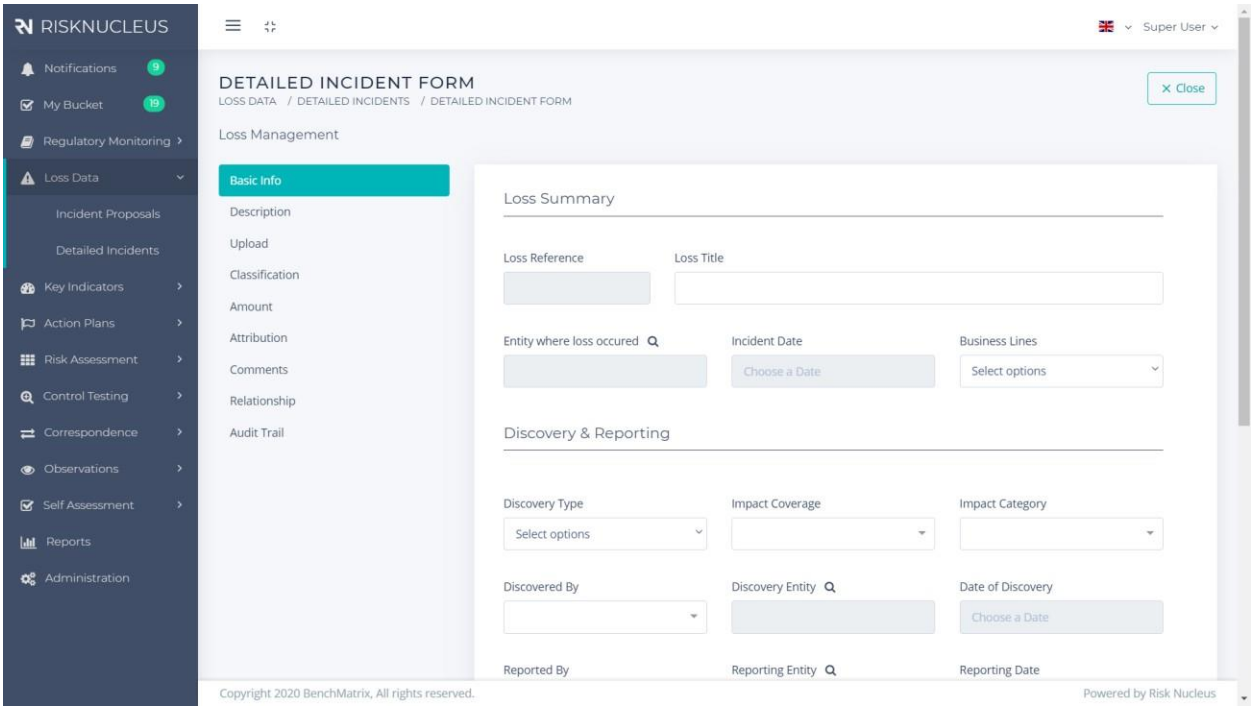


Figure 4. 17 : New Detailed Incident

Following fields are required to be filled when adding a new incident proposal

Attribute	Description
Loss Reference	Unique attributes assigned by the system automatically for differentiation
Loss Title	Incident name or description.
Entity Where Loss Occurred	Enables the tagging of incident to a single entity in the system
Incident Date	Refers to the date the incident originally occurred.
Business Lines	Refers to the business line the incident pertains to.
Discovery Type	Refers to how the discovery occurred. For example through Shariah Audit, etc.
Impact Coverage	Tagging the incident impact either as Isolated or Linked.
Impact Category	Refers to the category of the impact, for example, High, Medium, Low, Media, Regulatory, etc.
Discovered By	Tagging of the individual that discovered the incident.
Discovery Entity	Refers to the system entity that discovered the incident.
Date of Discovery	Refers to the date the incident was discovered.
Reported By	Tagging of the individual that reported the incident.
Reporting Entity	Refers to the system entity that reported the incident.
Date of Reporting	Refers to the date the incident was reported.
Group Wide Impact	Enables the marking of incident as having a group wide impact, Yes or No.
Credit/Market	Refers to the nature of impact in terms of Credit or Market or both.
Individual Involved	Refers to the individual involved in the incident.
Responsible Department	Refers to the department responsible for the incident.
Regulatory	Marking the incident as a regulatory incident, Yes or No.

Other Tabs

Tab Name	Functionality & Purpose
Description	Enables input of further details and descriptions with regards to theincident.
Uploads	Enables upload of supporting documentary evidence and justificationsof incident as relevant.
Classification	Enables categorization of incident according to its features and characteristics.
Amount	Enables the setting of a monetary value incurred as loss against the incident as required.
Attribution	Enables the attribution of the loss as required
Comments	Enables additional comments on the specific incident as necessary by workflow participants.
Action Plan	Enables linkage of incident with an appropriate action plan as required
Relationship	Enables the linkage of incident with other system modules as necessary.
Audit Trail	All actions performed and changes are recorded under this tab.

4.4 Risk & Control Self-Assessment

This chapter outlines the key functionalities of the RCSA module of the application. Thecontents are divided into following sections:

- ***Introduction***
- ***Risk Appetite Matrices Creation***
- ***Risk Register***
- ***Control Register***
- ***Risk Assessment***
- ***RCSA Workshop***
- ***Heat maps***

4.4.1 Introduction

RCSA is a process of identifying key risks of an organization and systematically addressing those risks by deployment of adequate controls for adequate risk targets. This entire process requires integration with various components of operational risk management and is effectivethrough decentralization of risk mitigation and control assurance activities.

The application RCSA Module enables identification of key risks and controls within the business, assess impact and likelihood for each risk, evaluate the risk exposure; score the design, performance and rigor of controls, and submit the assessments for review and appropriate management action.

4.4.2 Risk Register

The application RCSA Module has the functionality of a Risk Register which is the whole record/register of all risks as part of the database. This register can be viewed and results can befiltered as needed.

Note: This listing is hierarchy-bound therefore only those risks will be displayed in this screen that are associated with the entities of which the logged-in user has the hierarchy rights. **Hierarchy Rights** can be changed by Administrator from the administration screen.

In order to access this screen, following steps are required:

1. On the navigation bar, click on the **Risk Assessment** label to open the drop down list
2. Select and Click the **Risk Register** option to open the window.

Note: Only pages to which you have access rights appear in the menu. Access rights can be configured through the **User Rights configuration** page.

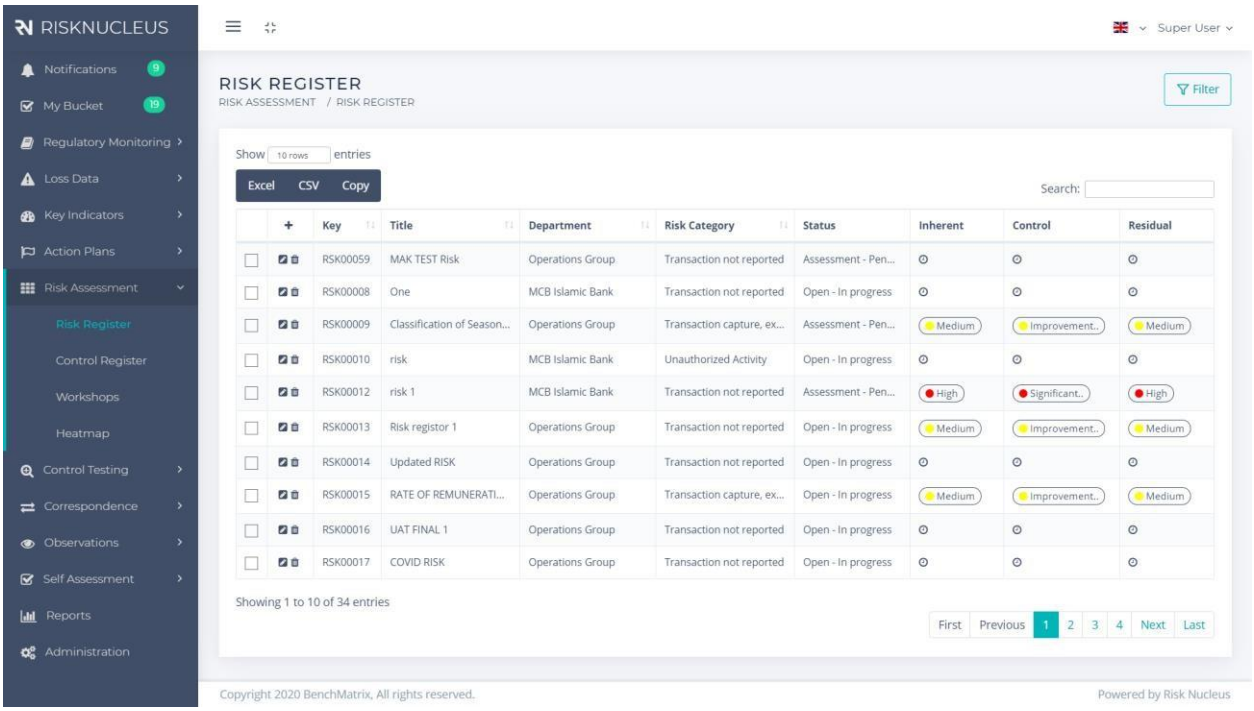


Figure 4. 18 : Risk Register

The application RCSA Module, enables the creation of new risks, once identified to be added tothe register for appropriate subsequent actions.

To add a new risk, follow the steps below:

1. On the navigation bar, click on the **Risk Assessment** label to open the drop down list
2. Select and Click the **Risk Register** option to open the window
3. Press the "+" button on the header row of the listing grid
4. Risk Addition window opens.

Note: Only pages to which you have access rights appear in the menu. Access rights can be configured through the **User Rights configuration** page.

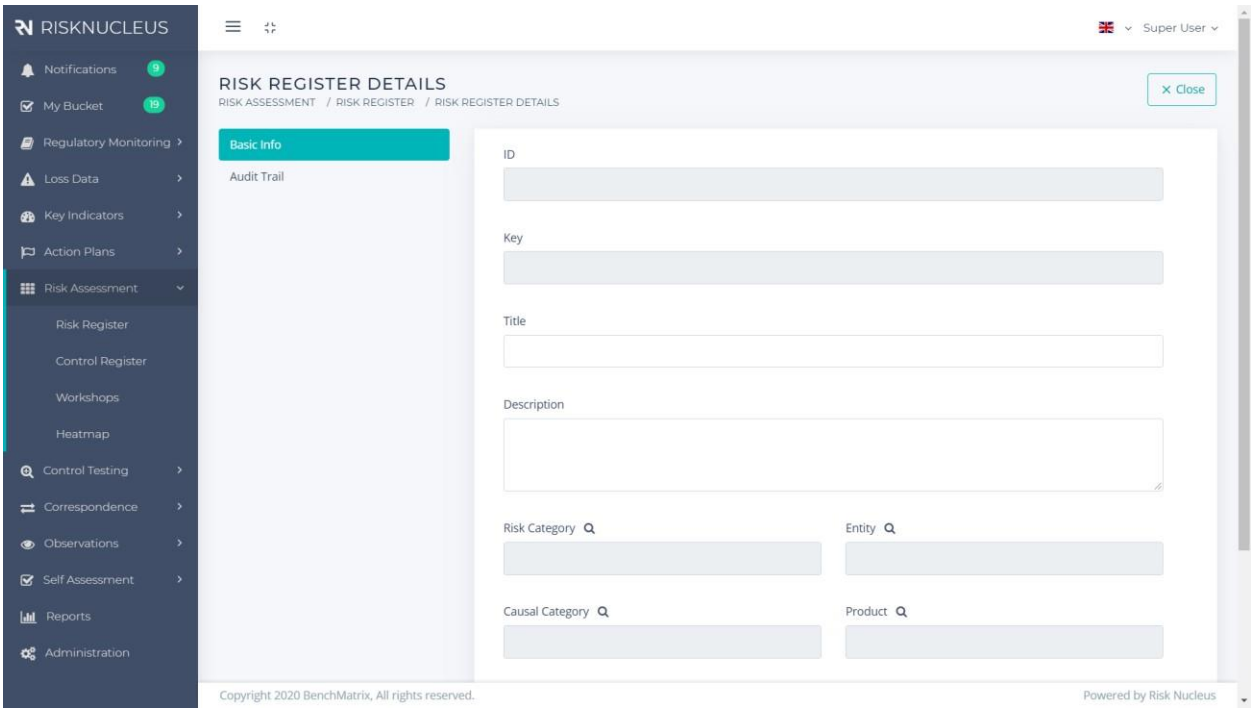


Figure 4. 19 : New Risk Addition

Following fields are required to be filled when adding a new risk:

Attribute	Description
ID & Key	**Unique attributes assigned by the system automatically for differentiation**
Title	Defines the subject of the risk
Description	Complete details regarding the risk
Risk Category	Refers to classification of risk
Entity	The business unit to which the risk pertains
Causal Category	Defines cause of risk occurrence
Product	The segment of business to which the risk pertains
Process	Business process linked to the risk
Risk Type	Refers to the broad classification of risk with respect to risk area

4.4.3 Risk Assessment

Risk assessment process is an integral element for any compliance function. This process can be defined as a tool to identify, classify, evaluate and work towards risk mitigation. As regulatory requirements are updated in the system, new risks are also identified pertaining to these. For allrequirements where a risk is identified, inherent risk assessment is performed while the controlsare incorporated and residual risk is calculated. This process is repeated for the annual RCSA exercise. Whereby both the risk and control assessments are reviewed and necessary changes are made as required.

Once a risk has been created, it will be visible in the list appearing on the risk register main page. The application RCSA enables risk assessment of all new and existing risks. In order toperform risk assessment using multiple variables, following steps are required:

1. Go to **Risk Assessment Tab** on the navigation bar
2. Select **Risk Register** drop down from the available options
3. Click on the title of respective risk appearing on the main risk register page
4. A new window will open where risk assessment can be performed along with multipleoptions for in depth assessment.

Note: Only pages to which you have access rights appear in the menu. Access rights can be configured through the **User Rights configuration** page.

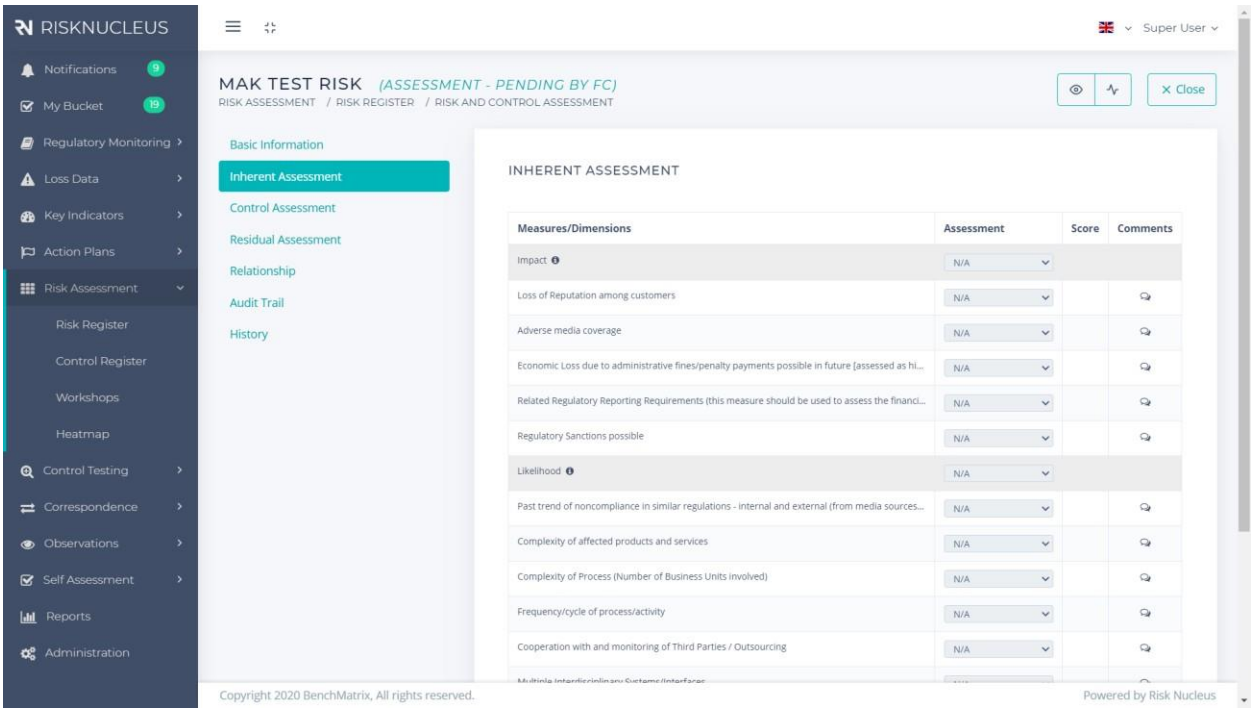


Figure 4. 20 : Risk Assessment

4.4.4 Control Register

The application RCSA Module has the functionality of a Control Register which is the whole record/register of all controls as part of the database. The Control library used subsequently inrisk assessment and control testing process to identify the operating effectiveness of the controls.

In order to access this screen, following steps are required:

1. On the navigation bar, click on the **Risk Assessment** option
2. Select **Control Register** option from the label drop down

Note: Only pages to which you have access rights appear in the menu. Access rights can be configured through the **User Rights configuration** page.

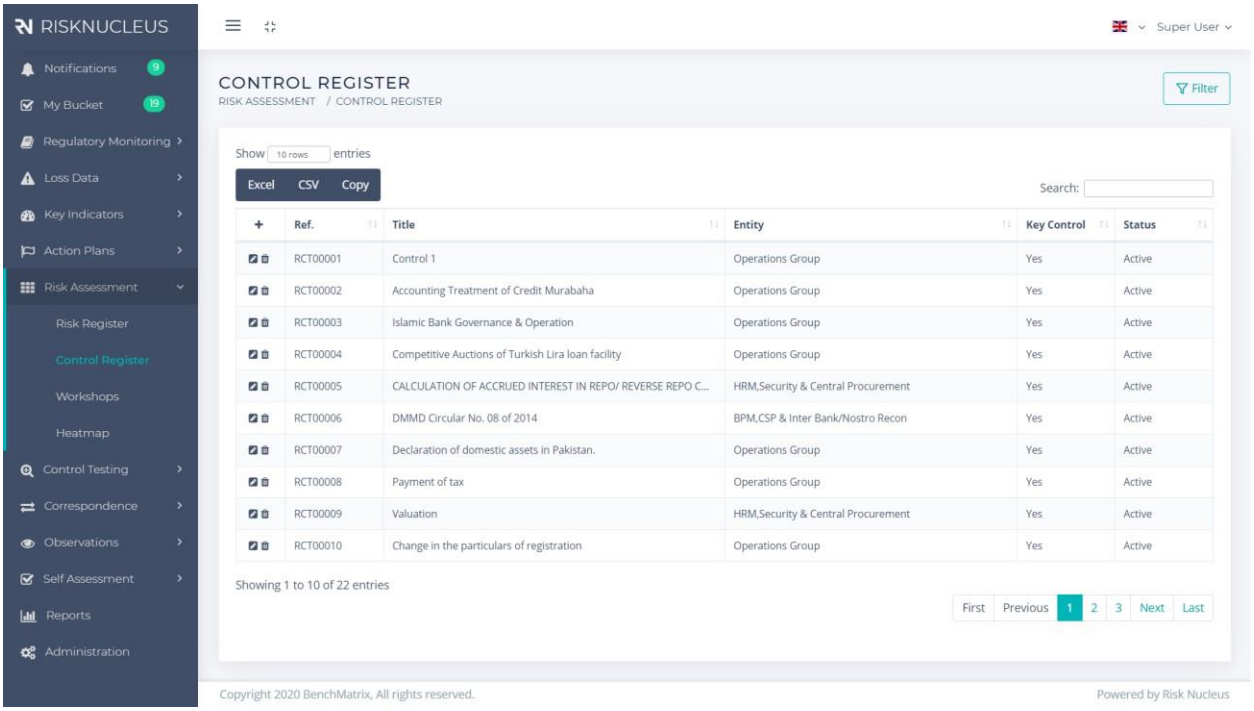


Figure 4. 21 : Control Register

4.4.5 Add Control

The application Risk Assessment Module, enables the creation of new controls, as required according to the risks identified & present in the Risk register for appropriate mitigation & subsequent actions.

To add a new control, follow the steps below:

1. On the navigation bar, click on the **Risk Assessment** label to open the drop down list
2. Select and Click the **Control Register** option to open the window
3. Press the "+" button on the header row of the listing grid
4. Risk Addition window opens.

Note: Only pages to which you have access rights appear in the menu. Access rights can be configured through the **User Rights configuration** page.

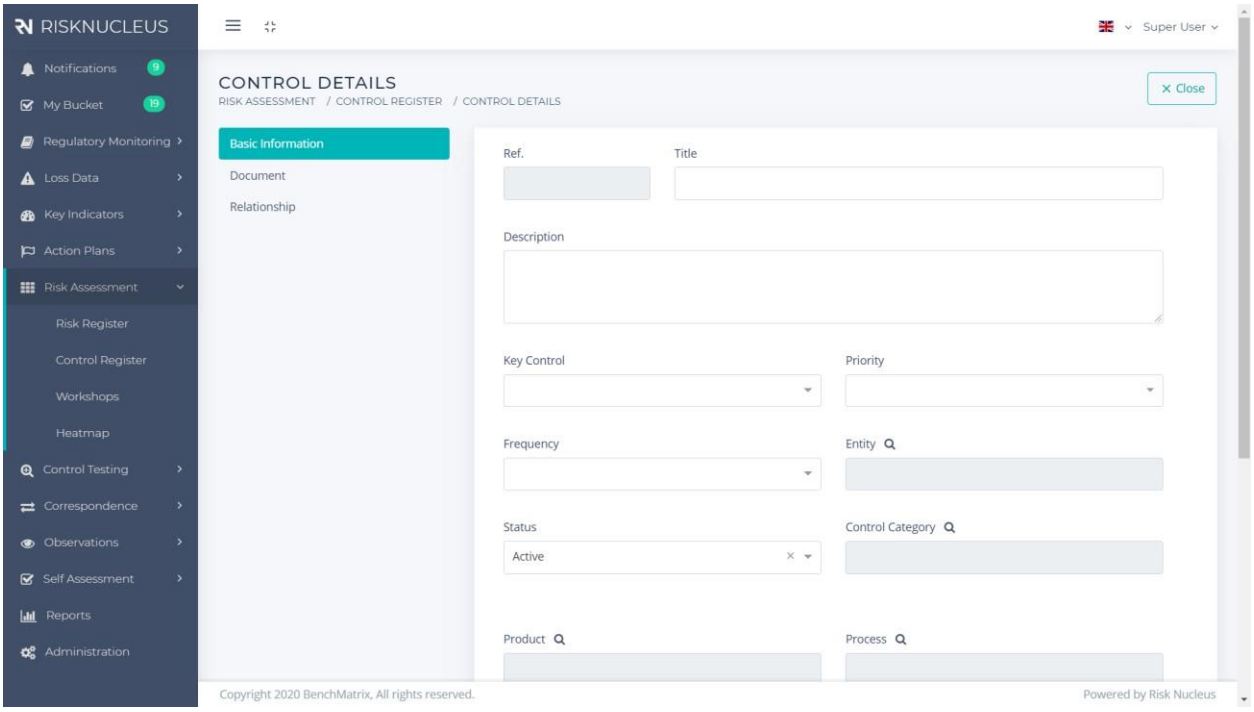


Figure 4. 22 : New Control Addition

Following fields are required to be filled when adding a new control

Attribute	Description
Reference	Unique attributes assigned by the system automatically for differentiation
Title	Defines the subject of the workshop
Description	Complete details regarding the workshop
Key Control	Option to mark new control as a Key Control or not.
Priority	Enables to mark control as Low, Medium or High priority.
Frequency	Sets the frequency of control, for example, daily, monthly, as required, etc.
Entity	Concerned department for the workshop
Status	Enables to mark control as active or In active
Control Category	Enables tagging of control category.
Product	Enables tagging of control to entity products.
Process	Enables tagging of control to entity processes.
COSO Category	Enables selection of COSO category for the control.
COSO Component	Enables selection of COSO component for the control.
COSO Control Classification	Enables Classification of control as under COSO.
Control Type	Enables tagging of control type.
COSO Financial Assertion	Enables selection of COSO financial assertion for control.

Other Tabs

Tab Name	Functionality & Purpose
Documents	Supporting documents or the original documentary evidence relating toa requirement as received from the regulator can be uploaded here.
Audit Trail	All actions performed and changes are recorded under this tab.

4.4.6 Risk Appetite Matrices Creation

The Risk Appetite Matrices (RAM) option allows the user to create multiple Risk Appetite Matrices and link them to specific departments in the organization. The risks in each department shall be assessed using the parameters of the RAM that is linked to the respective department.

In order to access this screen, following steps are required:

1. On the navigation bar, click on the **Administration** label to open the window
2. Scroll down to RCSA section
3. Choose **Risk and Control Assessment Definition**

Note: Only pages to which you have access rights appear in the menu. Access rights can be configured through the **User Rights configuration** page.

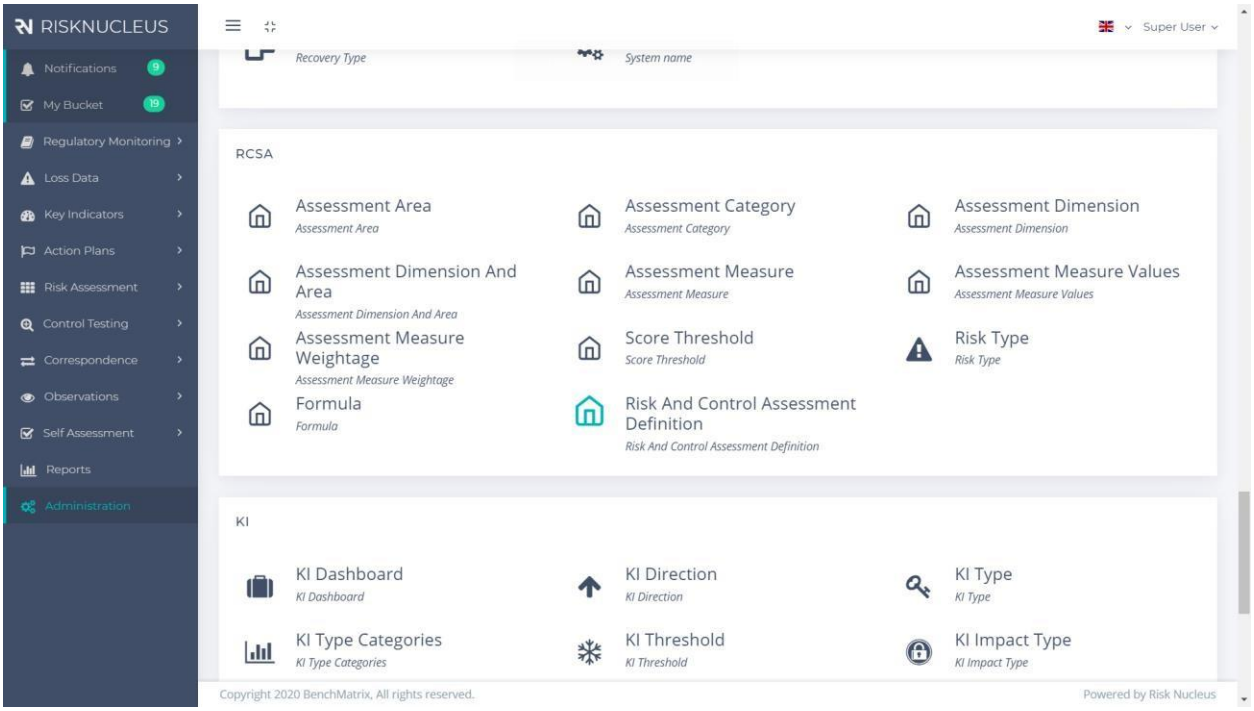


Figure 4. 23 : RAM Creation Access

RAMs are added by clicking on the + icon on the top left box of the Risk and Control Assessment Definition page. To create a RAM, the user will name the RAM and link it to an entity within the business. In case the user links the RAM to the top most entity in the business hierarchy, this RAM will serve as a bank-wide RAM that can be used for assessment of all risks.

4.5 Heat Map

The main purpose of this screen is to display inherent and residual values of risks on heat maps.Heat map depicts the plotting of risk and calculate the aggregate score of risk on the basis of configured risk appetite matrix. The user can filter the graphs through the available filters on top of the screen.

In order to access the Heat Map screen, following steps are required.

1. On the navigation bar, click on the **Risk Assessment** option
2. Select **Heat Map** option from the label drop down

   Note: Only pages to which you have access rights appear in the menu. Access rights can be configured through the **User Rights configuration** page.



Figure 4. 24 : Heat Maps

4.6 Key Indicators

This chapter outlines the key functionalities of the Key Indicators module of the application.The contents are divided into following sections:

- ***Introduction***
- ***Data Points***
- ***Input***
- ***Key Indicators***
- ***Dashboard***

4.6.1 Introduction

Key Indicators are an integral part of any risk management process. They serve as clear signalsof risk and can be measured to judge the effectiveness of controls. Selection of appropriate keyindicators is of paramount importance as your risk management is only as strong as the Key indicators chosen. The application Key Indicators module provides the user with enhanced customization and functionality in terms of setting Key indicators, selecting data points and also enables users toupload data into the system manually through input facility. Downloadable templates are provided for guidance and users are also free to create their own templates for data input.

The application Key Indicators module ensures that the user has all the information needed toselect the most transparent Key indicators to strengthen their risk management process.

4.6.2 Data Points

Data points are used to provide indications as required for key indicators. These data points are used to measure risks and control effectiveness within the system.

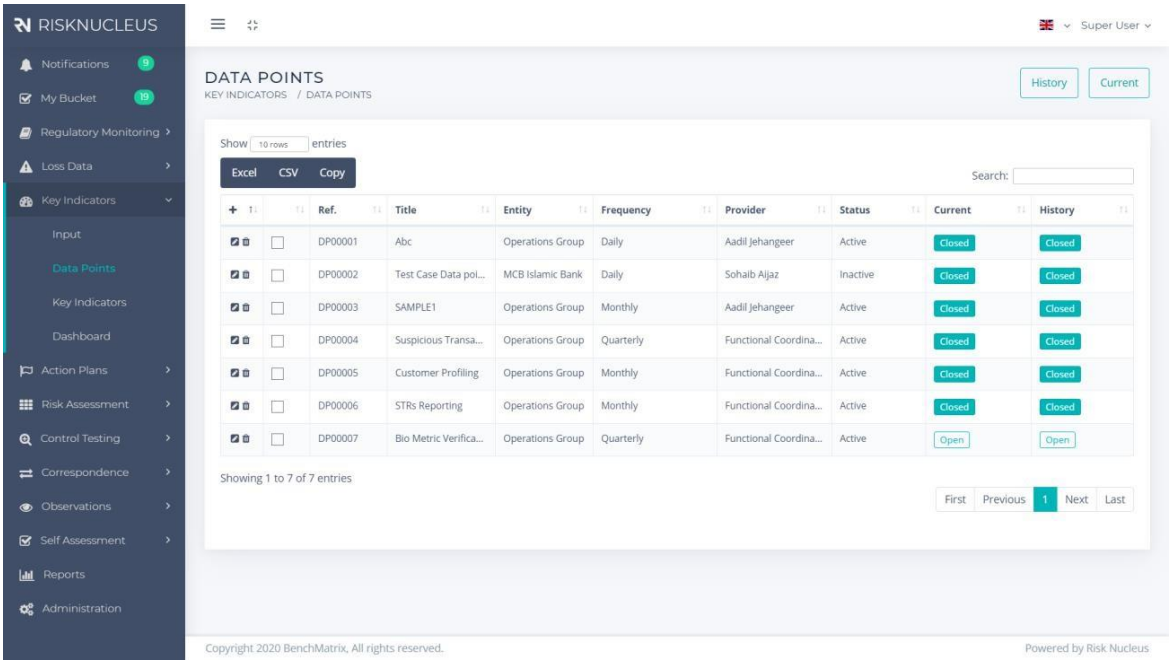


Figure 4. 25 : Data Points

Data points lists down all existing data points in the system. Users have the option to switch viewbetween historical data points and current data points presented within the listing grid. Users can search data points at their convenience and data points listing grid can be downloaded in various formats for easy and accessibility.

4.6.2.1 Adding New Data Points

The application Key Indicators module provides the functionality of adding new data points asrequired by users.

To add a new Input, follow the steps below:

1. On the navigation bar, click on the **Key Indicator** label to open the drop down list
2. Select and Click the **Data Points** option to open the window
3. Press the "+" button on the header row of the listing grid
4. New Data Points window opens.

Note: Only pages to which you have access rights appear in the menu. Access rights can be configured through the **User Rights configuration** page.

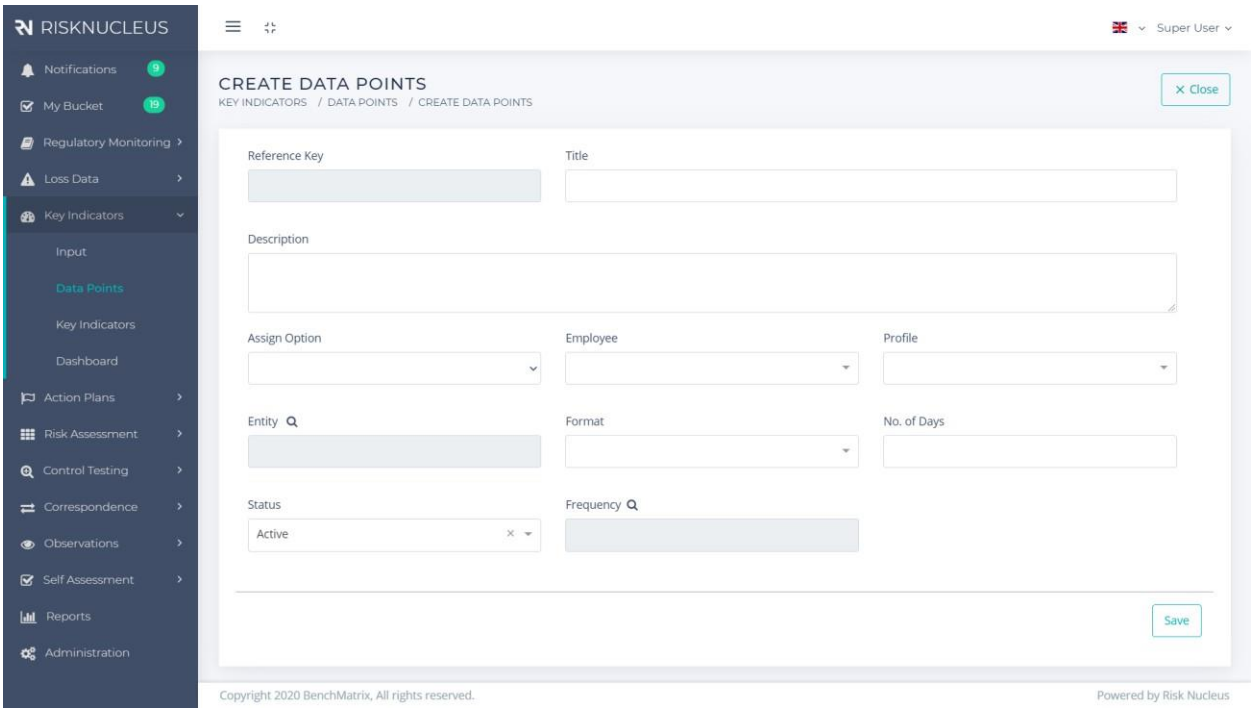


Figure 4. 26 : Create New Data Points

Following fields are required to be filled when adding a new data point.

Note that data point frequency and deadline must be Xerox of linked Key indicator frequencyand deadline

Attribute	Description
Reference Key	Unique attributes assigned by the system automatically for differentiation
Title	Refers to the title of the Data Point.
Description	Data Point description.
Assign Option	Option available to assign data point either to a specific employee or toa system profile.
Employee	Enables the tagging of relevant employee to the data point if assigned.
Profile	Enables the tagging of relevant system profile to the data point if assigned.
Entity	Enables the tagging of relevant system entity with the control plan.
Format	Refers to the format of the data point
No. of Days	Refers to the number of days over which the data point will be recorded
Status	Enables marking of data point as either Active or Inactive
Frequency	Enables the setting of frequency for the data point.

4.6.3 Input

Input screen is provided to enable users to upload data manually for key indicator measurement. Data point template is downloadable for user convenience. Input window listsdown all previous data points uploaded with details regarding value, frequency, cycle and closure dates all available at a glance.

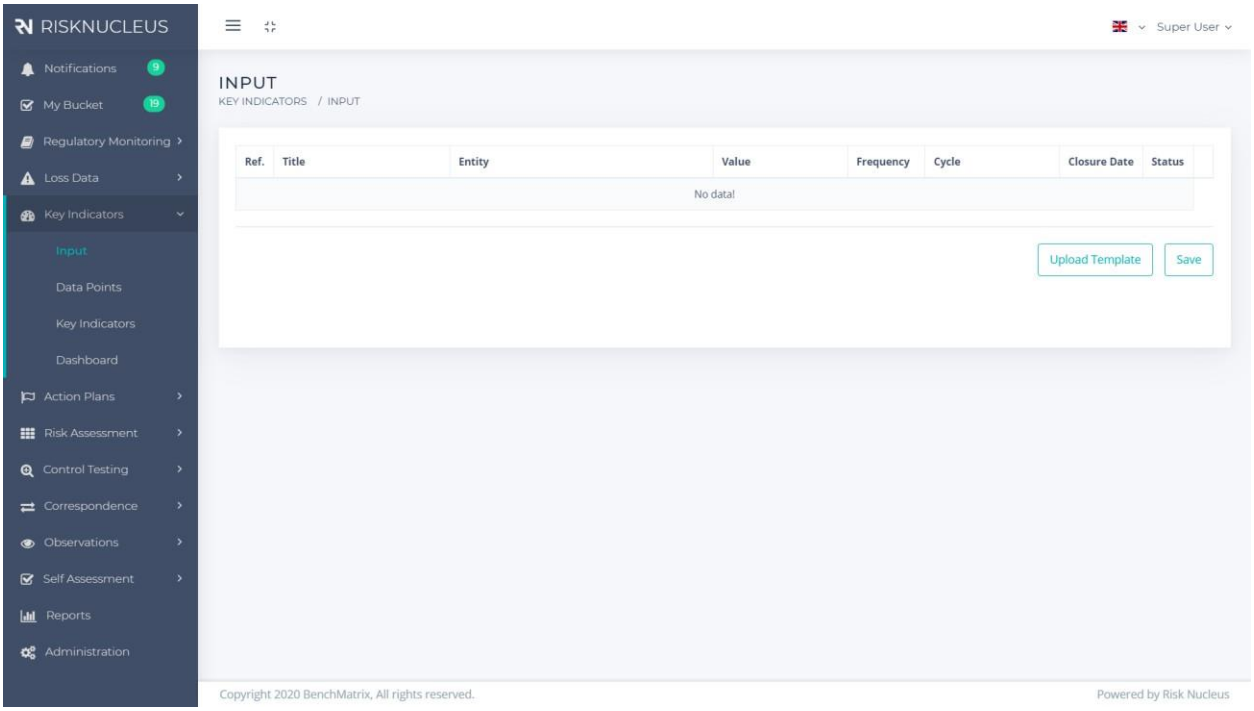


Figure 4. 27 : Input Page

4.6.3.1 Adding New Input

To add a new Input, follow the steps below:

1. On the navigation bar, click on the **Key Indicator** label to open the drop down list
2. Select and Click the **Input** option to open the window
3. Press the **Upload Template** button at the bottom of the grid
4. Upload Data Point Value widow opens.

Note: Only pages to which you have access rights appear in the menu. Access rights can be configured through the **User Rights configuration** page.

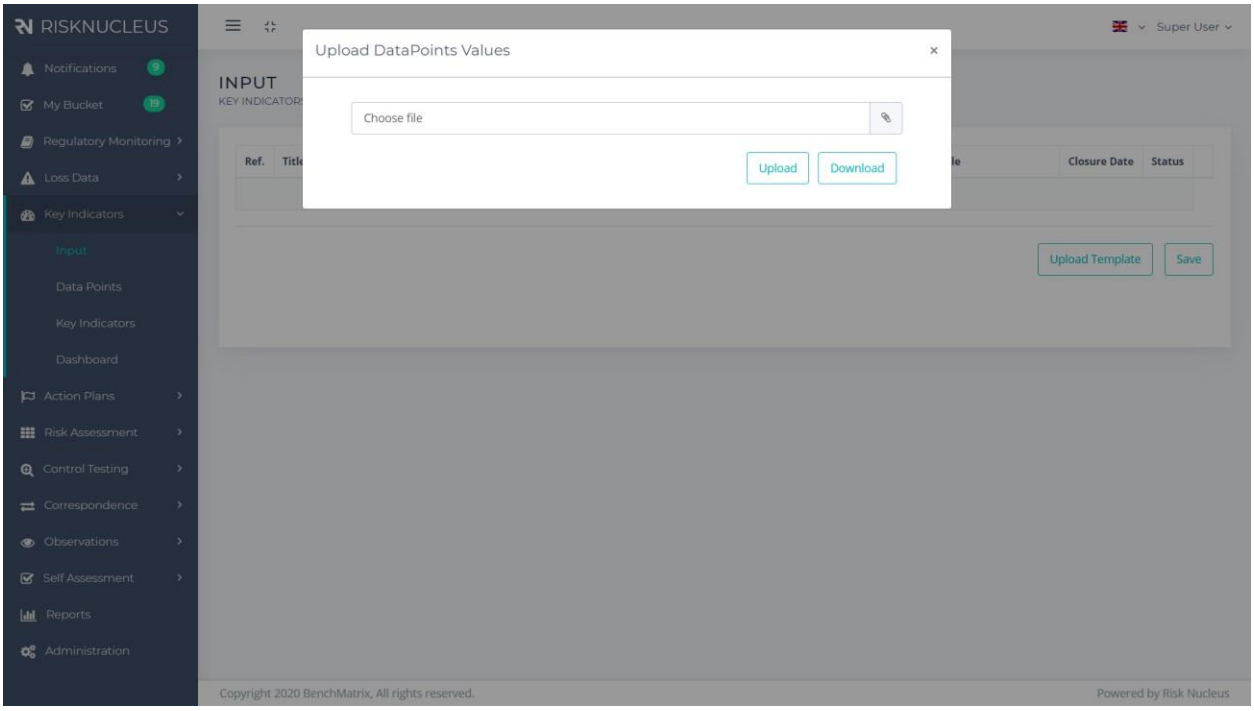


Figure 4. 28 : New Input

4.6.4 Key Indicators

Key Indicators provides users with a listing grid of all key indicators currently present in the system along with their details. Users can filter their view according to entity and or business plans. The listing grid is also downloadable in multiple formats for user convenience. Existing key indicators can also be edited through the grid as needed.

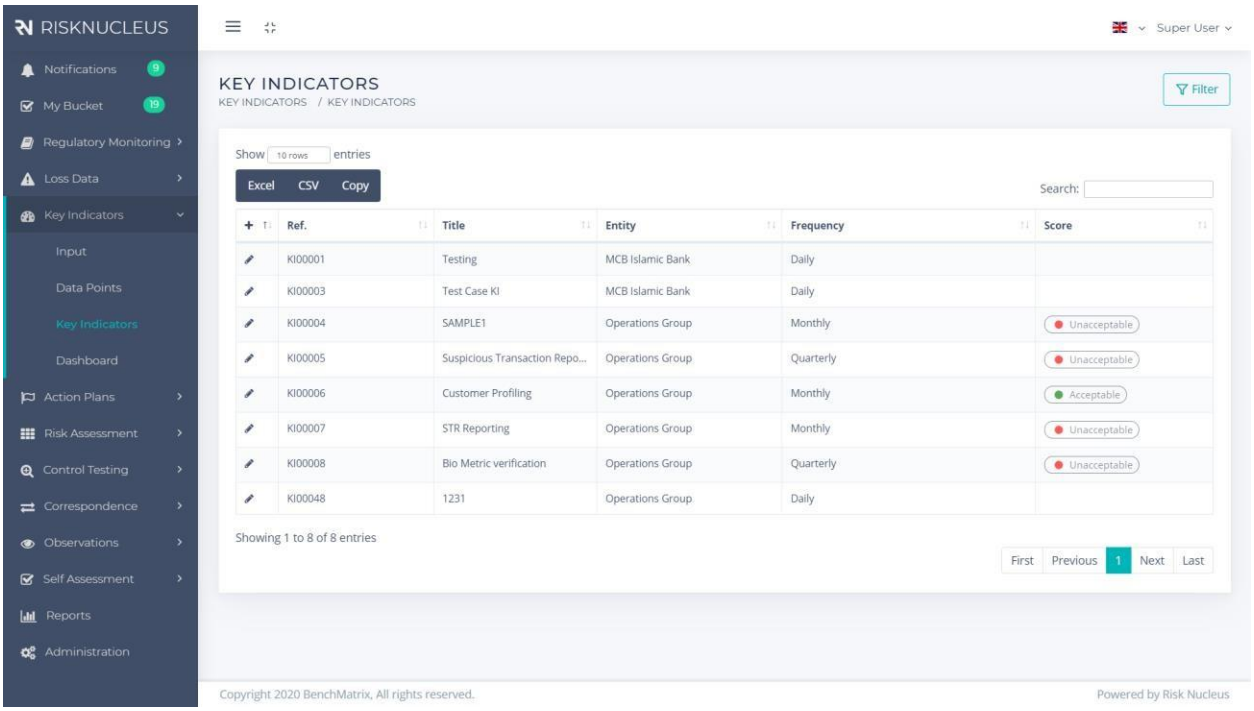


Figure 4. 29 : Key Indicators

4.6.4.1 Adding New Key Indicators

The application Key Indicators module provides the functionality of adding new key indicatorsas required by users.

To add a new Input, follow the steps below:

1. On the navigation bar, click on the **Key Indicator** label to open the drop down list
2. Select and Click the **Key Indicator** option to open the window
3. Press the "+" button on the header row of the listing grid
4. New Key Indicator window opens.

Note: Only pages to which you have access rights appear in the menu. Access rights can be configured through the **User Rights configuration** page.

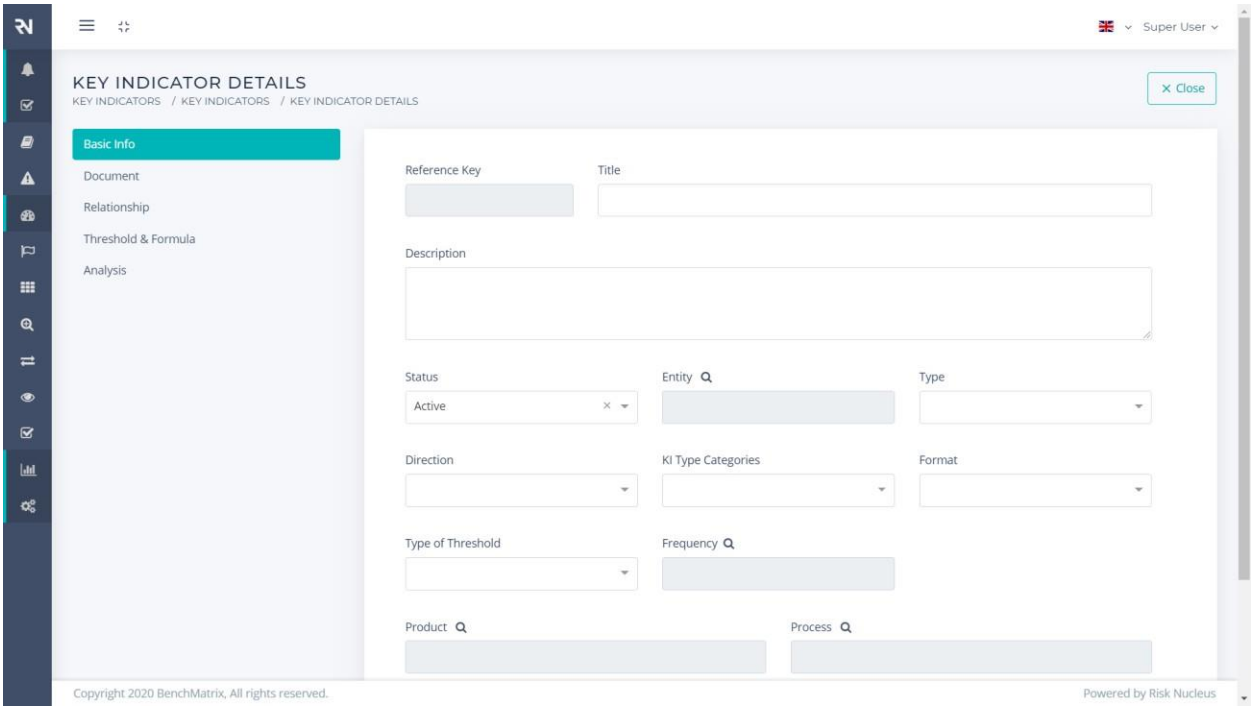


Figure 4. 30 : New Key Indicators

Following fields are required to be filled when adding a new key indicator

Note: Data point frequency and deadline must be Xerox of linked Key indicator frequency anddeadline

Attribute	Description
Reference Key	Unique attributes assigned by the system automatically fordifferentiation
Title	Refers to the title of the Key Indicator.
Description	Key Indicator description.
Status	Enables marking of Key Indicator as either Active or Inactive
Entity	Enables the tagging of relevant system entity with the Key Indicator.
Type	Refers to the type of key indicator, either one of People, Process or System.
Direction	Refers to the direction of the Indicator, either leading or lagging
KI Type Categories	Refers to the category type of Key indicator, choose from Top, Generic or Business specific.
Format	Refers to the format of the Key Indicator.
Type of Threshold	Refers to the type of threshold. Either Higher is worse or Lower is worse.
Frequency	Enables the setting of frequency for the Key Indicator.
Product	Enables the tagging of the Key Indicator to different products, multiple options can be selected.
Process	Enables the tagging of the Key Indicator to different processes, multiple options can be selected.

Other Tabs

Tab Name	Functionality & Purpose
Document	Enables attachments and other relevant document uploads for justifications as needed.
Relationships	Enables the linkage of the questionnaire with certain rules, regulations, activities, controls and other modules as relevant.
Threshold	Enables users to set thresholds for the key indicators.
Formula	Enables users to manually enter calculation formulas as appropriate.
Analysis	Provides graphical representation of the key indicator and linked datapoints

4.6.5 Dashboard

Once key indicators are created and data points are set, the dashboard functionality providesusers graphical representation of the Key indicators and their current status, along with risk weightage and other details.

Dashboards are categorized department wise, these departments are the same as mentioned under key indicators. Along with the graphical visualization, this window also shows linkedkey indicators for the department along with their trends and values within a listing grid.

The application Administration module provides users the functionality to create newDashboards as required for various key indicators under different departments.

1/. To create a new dashboard, visit the Administration module under KI section.

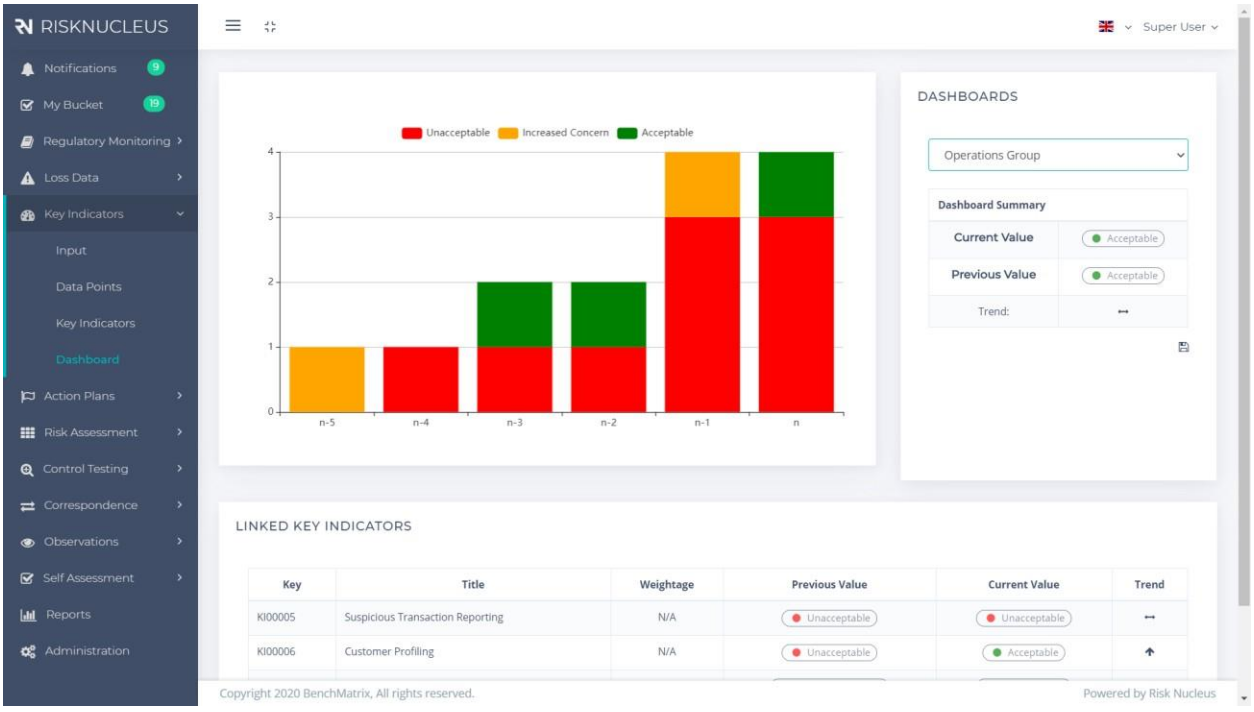


Figure 4. 31 : Dashboards

4.7 Action Plans

This chapter outlines the key functionalities of the Observations module of the application. Thecontents are divided into following sections:

- ***Introduction***
- ***Manage Action Plans***

4.7.1 Introduction

Action plans are necessary to avoid repetition of any loss making incident as well as to ensure compliance. Action plans provide a substantial course of action to rectify any errors in the process or system or to fix these as necessary to avoid further loss making events. The application Action Plan module provides users the functionality to view and monitor the progress of allcurrent action plans, create and edit new action plans as required and link action plans to incidents to ensure compliance and avoid repetition.

4.7.2 Manage Action Plans

This window gives users a listing grid view of all current action plans with their current statusand other details. Users can search and filter their view as required, while action plans can alsobe downloaded in multiple formats for accessibility.

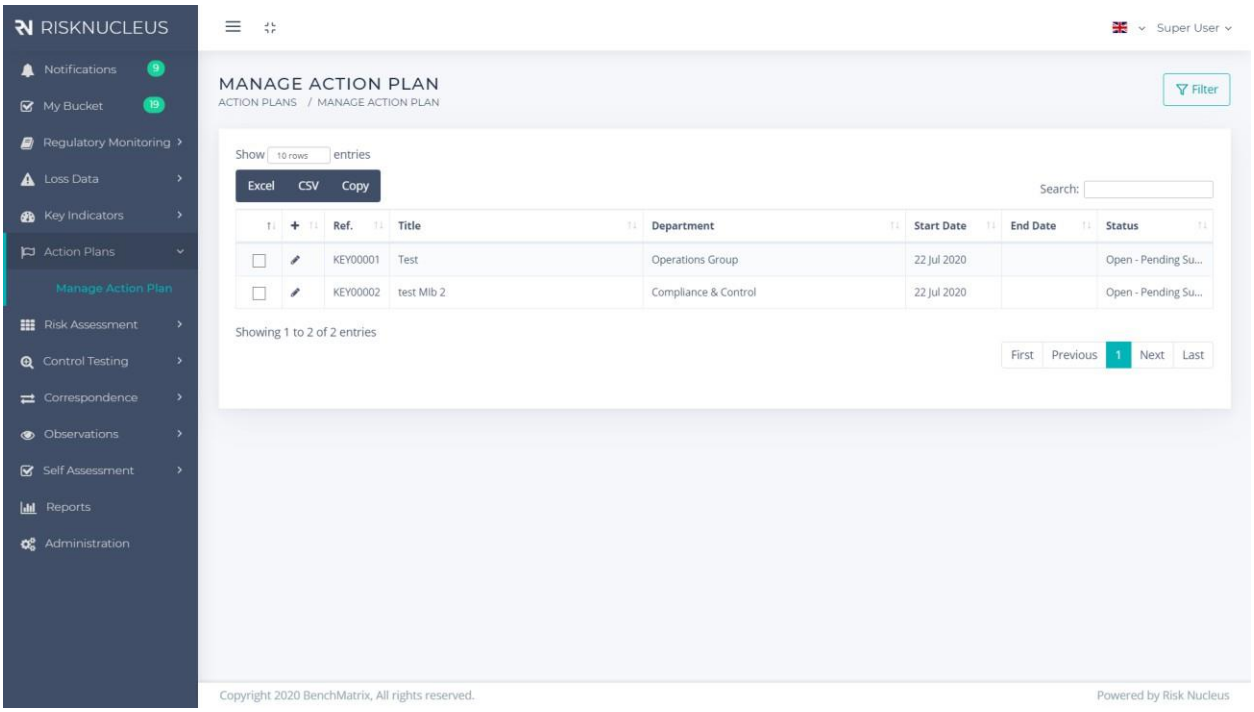


Figure 4. 32 : Manage Action Plans

4.7.2.1 Adding New Action Plans

The application Action Plans module provides the functionality of adding new key indicators asrequired by users.

To add a new Input, follow the steps below:

1. On the navigation bar, click on the **Action Plan** label to open the drop down list
2. Select and Click the **Manage Action Plans** option to open the window
3. Press the "+" button on the header row of the listing grid
4. New Action Plan window opens.

Note: Only pages to which you have access rights appear in the menu. Access rights can be configured through the **User Rights configuration** page.

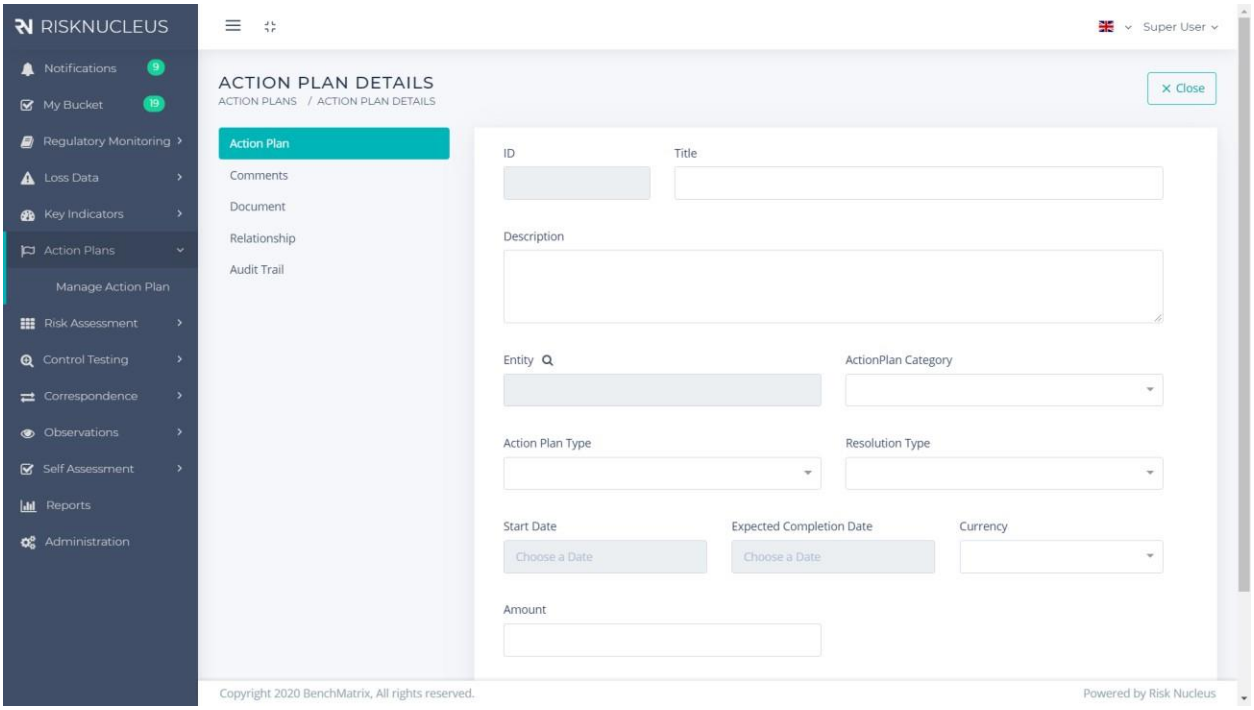


Figure 4. 33 : New Action Plan

Following fields are required to be filled when adding a new action plan

Attribute	Description
ID	Unique attributes assigned by the system automatically fordifferentiation
Title	Refers to the title of the Action Plan.
Description	Action Plan description.
Entity	Enables the tagging of relevant system entity with the Action Plan.
Action Plan Category	Refers to the category of the action plan, whether it's a for a Key Indicator, Observation, Control or Risk Assessment.
Action Plan Type	Refers to the type of action plan, either corrective or preventive.
Resolution Type	Refers to the outcome of the action plan, either a Temporary Fix or a Permanent Fix
Start Date	Enables the setting of a start date for the Action Plan.
Expected Completion Date	Enables the setting of an expected completion date for the Action Plan
Currency	Enables setting of currency for Action Plan
Amount	Enables setting amount in selected currency for Action Plan.

Other Tabs

Tab Name	Functionality & Purpose
Comments	Enables addition of comments on the action plan by relevant users.
Documents	Enables attachments and other relevant documents to be uploaded for justification of action plan as required.
Relationships	Enables the linkage of the action plan with other modules as required.
Audit Trail	Enables a digital record of all changes and additions to the action plansince creation.

General Conclusion

5 Conclusion

The Advanced Measurement Model - AMM is the most complex method of calculating the minimum capital requirement for operational risks and involves the elaboration of internal models, being used, generally, by internationally active banks, which are part of a group of financial institutions, and in which this thesis covered its automation by implementing the ORM application.

The development objective following the above model and gathering the complete package of operational risk management including loss data collection, risk and control self assessment (starting by risk and control identification to the actual risk assessment), key risk indicators and action plans has been completely attended by utilizing the most recent frameworks dedicated for web development.

Going through the implementation of each corner of operational risk management, revealed the lid about a facinated deployment that suits the cross module this application was based on by entering the orchastration world modern cloud servers are leading to, and therefore steps can be taken ahead to these servers ,such as kubernetees on AWS, google clouds or azure, by reflecting the minimized executable image to them.

6 References

[1] J. Lindvall, “Operational Risk Management Improvements within Internal Control Frameworks Nazanin Bagherzadeh Kateryna Jöehrs.”

[2] “Risk Management - A Basic Understanding.” https://www.managementstudyguide.com/risk-management.htm (accessed Jun. 15, 2022).

[3] “Operational Risk: Definition and Drivers.” https://www.managementstudyguide.com/operational-risk.htm (accessed Jun. 15, 2022).

[4] “Identification of Operational Risks.” https://www.managementstudyguide.com/identification-of-operational-risks.htm (accessed Jun. 15, 2022).

[5] “Operational Risk Management - Opportunities and Challenges Beyond Basel II - The Global Treasurer.” https://www.theglobaltreasurer.com/2007/01/22/operational-risk-management-opportunities-and-challenges-beyond-basel-ii/?amp=1 (accessed Jun. 15, 2022).

[6] “How to Identify Operational Risks.” https://www.managementstudyguide.com/how-to-identify-operational-risks.htm (accessed Jun. 15, 2022).

[7] “Using Internal Loss Data to Mitigate Operational Risks.” https://www.managementstudyguide.com/using-internal-loss-data-to-mitigate-operational-risks.htm (accessed Jun. 15, 2022).

[8] “External Loss Data in Operational Risk Management.” https://www.managementstudyguide.com/external-loss-data-in-operational-risk-management.htm (accessed Jun. 15, 2022).

[9] “Risk Control Self Assessment (RCSA).” https://www.managementstudyguide.com/risk-control-self-assessment.htm (accessed Jun. 15, 2022).

[10] “Key Risk Indicators.” https://www.managementstudyguide.com/key-risk-indicators.htm (accessed Jun. 15, 2022).

[11] “Various-units-are-combined-to-build-an-angular-application.jpg (692×412).” https://www.tutorialandexample.com/wp-content/uploads/2019/07/Various-units-are-combined-to-build-an-angular-application.jpg (accessed Jun. 15, 2022).

[12] “Spring Boot Tutorial.” https://www.tutorialspoint.com/spring_boot/index.htm (accessed Jun. 15, 2022).

[13] “What is API: Definition, Specifications, Types, Documentation | AltexSoft.” https://www.altexsoft.com/blog/engineering/what-is-api-definition-types-specifications-documentation/ (accessed Jun. 15, 2022).

[14] “Design Patterns.” https://sourcemaking.com/design_patterns (accessed Jun. 15, 2022).

[15] “Design Patterns used in Spring Framework | JavaInUse.” https://www.javainuse.com/spring/spring-design-patterns (accessed Jun. 15, 2022).

[16] “Integrating Hibernate and JPA with Spring Boot – Spring Boot Tutorial.” https://www.springboottutorial.com/hibernate-jpa-tutorial-with-spring-boot-starter-jpa (accessed Jun. 15, 2022).

[17] “Java Mail Tutorial- javatpoint.” https://www.javatpoint.com/java-mail-api-tutorial (accessed Jun. 18, 2022).

[18] “What is Redis Cache? Redis Cache Explained Simply [2022] | Nexcess.” https://www.nexcess.net/blog/what-is-redis-cache/ (accessed Jun. 15, 2022).

[19] “redis-how-it-works.png (980×660).” https://linuxiac.b-cdn.net/wp-content/uploads/2021/06/redis-how-it-works.png (accessed Jun. 15, 2022).
[20] “Spring Boot - OAuth2 with JWT.” https://www.tutorialspoint.com/spring_boot/spring_boot_oauth2_with_jwt.htm (accessed Jun. 18, 2022).
[21] “Microservices-vs-monolithic-architecture-diagram.png (800×600).” https://avinetworks.com/wp-content/uploads/2018/06/Microservices-vs-monolithic-architecture-diagram.png (accessed Jun. 15, 2022).