Access Control Process for a SaaS Provider

UNIVERSITY OF TURKU
Department of Future Technologies
Master of Science in Technology Thesis
June 2019
Syeda Nazish Kazmi

Supervisors:
Seppo Virtanen
Petri Sainio

UNIVERSITY OF TURKU
Department of Future Technologies

Syeda Nazish Kazmi: Access Control Process for a SaaS Provider

Master of Science in Technology Thesis, 90 p.
Security of Networked Systems
June 2019

Access control is a process of limiting access to systems and services. It is a way by which the users are granted access and privileges to information and resources of an organization. The process involves controlling, managing, logging and reviewing access. It ensures that individuals in an organization are able to access and use the systems they need to do their job but do not have more than the needed access.

An organization's major asset is the information regarding customers, processes, products, and suppliers which are critical for its operations. The internet-based technologies provide integration of corporate applications, internal and third-party systems, decision support systems, knowledge management, and repositories. The most common threat to these critical resources is unauthorized access that can pave ways for malicious activities that are harmful and can lead to loss of confidentiality, integrity, and availability. In order to minimize the risks and ensure business continuity, access control process following the best practices should be in place.

In this thesis an access control process for a SaaS organization is designed, implemented and tested. Protection of the proprietary information and resources is of prime importance for such an organization. The existing access control process is not following industry standards and best practices. As the organization is growing fast, the business and organizational requirements are also changing. In order to comply with standards for access control, the new access control process is carried out as per the guidelines provided by security standards while keeping in view the growing organization needs. All controls have been designed as per the requirements of SOC 2 and ISO 27001. The process is implemented mainly on the basis of role-based access (RBAC) model and the principle of “need to know”.

Client satisfaction, legal harmonization, and financial returns are among the benefits that the organization gets by having an access control process in line with security standards. Moreover, the organization is not only able to prevent data breaches but also meet the regional and worldwide regulations.

Keywords: access control, role-based access, least privilege, security standards.

Acknowledgement

I would like to acknowledge everyone who has played a role in my academic accomplishment. First of all, I thank the organization and the project manager for believing in me and providing the opportunity to work on this project. My sincere gratitude to Dr. Seppo Virtanen for his active guidance, cooperation, and help. I am immensely grateful to my colleagues who have always helped and guided me throughout the project. Personally, I thank my parents and fiancé for their constant support and encouragement through this incredible journey.

Table of Contents

Abbreviations and Acronyms

ACL	Access Control List
COSO	Committee of Sponsoring Organization
DAC	Discretionary Access Control
ESMS	Enterprise Security Management System
IAMS	Identity and Access Management System
IITS	Internal IT Support
ISO	International Organization for Standardization
MAC	Mandatory Access Control
MFA	Multifactor Authentication
NIST	National Institute of Standards and Technology
RBAC	Role Based Access Control
SaaS	Software as a service
SAML	Security Assertion Markup Language
SOC	Service Organization Control
SoD	Separation of Duties

1 Introduction

In today's era, as technology becomes incorporated in our lives, businesses are continuously working on improving efficiency and productivity to stay ahead of the competition. Information storage, processing, transmission and integration provided by various technological devices is one of the most critical resources for conducting businesses. These capabilities offer many benefits to organizations including increased functionalities for users, rapid access to information, efficient service to customers, increased visibility to the outside world. However, such technologies also come with the cost of security threats and risks such as unauthorized access.

In this thesis, the case organization is a SaaS provider that deals with a lot of customer data and have several internal as well as third-party tools for product development and service provision. One of the prime concerns for such an organization is the logical access to data and resources. The existing access control process is not up to industry standards for an organization that is growing too fast. The new access control process is implemented to protect customer and organizational data, meet customer and growing organizational requirements and ensure business continuity. This is achieved by designing and implementing an access process that follows the standardized security framework best practices of ISO 27001 and SOC 2.

The thesis is organized in a way that relevant literature in access control domain and the objective of having a certified access control process in place has been discussed in the next chapter. Moreover, chapter 3 analyses the organizational systems that are involved in the process and the requirements of access control by security standards. In chapter 4, the access control process is designed while keeping in view the organizational and business requirements identified in chapter 3. Furthermore, the inclusion of existing users in the system, implementation, and testing of the access control process is discussed in the last chapter.

Chapter 2

2 Literature Review

This chapter provides an overview of the relevant work in the field of access control and some discussion about security standards. In section 2.1, we discuss some background of the access control process. Traditional access control models and the access control techniques that provide the enforcement mechanisms have been discussed in section 2.2 and 2.3 respectively. Moreover, in section 2.4 we discuss the basic components of access control planning. The Role-Based Access Control (RBAC), its models and security principles have been analyzed in section 2.5. Further, we examine the existing work related to the constraints in RBAC and its limitations. Section 2.6 discusses some related terms in the access control process and later the security standards and purpose of complying with the standards have been analyzed in section 2.7.

2.1 Access Control

Access control is defined as the process to grant or deny a request to use or obtain information and related services that involve information processing and obtain access to physical facilities (Kissel, 2013). Long before the modern computer era, the concept of access control existed. In the early 20th century, it was used in transportation for controlled access to highways and roads. Later, in 1964, one of the MIT projects described the concept of access control in the computer system and emphasized addressing the data protection issues in shared systems. The National Institute of Standards and Technology (NIST, 2014) states that information security access control should include following aspects: access control policy and procedures, account management, access enforcement, information flow enforcement, separation of duties, least privilege, data mining protection, access control decisions, and reference monitor.

Access control process determines the activities a user is authorized to perform and mediating the attempts of the user to access system resources. Access control systems can be implemented by an information technology infrastructure in various places and levels. Directories and files in operating systems are protected by using access control. Database management systems also regulate access to views and tables by access control.

Moreover, most of the commercially available applications independent of their OS and database management system on which they are installed, implement access control. Access control is implemented in most commercially available systems and mostly independent of the DBMS or underlying operating systems (Hu, Ferraiolo, & Kuhn, 2006).

The main objective of the access control process is expressed as only allowing legitimate access to system sources and protecting against any inappropriate or unauthorized access. This could be described as the optimal sharing of information from a business perspective. The important objective of IT is to make sharing and availability of information between users as easy as possible. Resource protection can become difficult with a greater degree of sharing but an access control mechanism that is effective and well managed eases sharing. Selective sharing of information is possible when the access control mechanism is sufficiently fine-grained else it is considered risky.

2.2 Access Control Models

Access control is one of the basic internal security controls in systems with shared access to resources. Many organizations including IT companies, hospitals, government, and educational institutions implement the access control mechanisms to protect information resources. It is the process of defining policies that determine the resources accessible by the subject i.e. process, user or computer and the operations they are allowed to perform on an object i.e. file, database, a table or service. Moreover, managing user privilege rights is one of the most challenging tasks in access control.

Several access control models have been proposed such as Discretionary (Lampson, 1974), Mandatory (Denning, 1976) and Role-based access control models (Sandhu et al.,1996). In the information security industry, among various models, MAC and DAC are widely implemented. RBAC has emerged as their alternative as it reduces the complexity and eases security management. Access model provides a framework that dictates the way subjects can access objects. It uses security mechanisms and access control technologies to enforce the objectives and rules of the access models. Alan O'Connor and Ross Loomis (2010) have discussed the main type of access models.

2.2.1 Discretionary Access Control Model

In the early 1970s, the discretionary access control model was proposed by Lampson (Lampson, 1974). In this model, the control of access in the discretionary access control model is based on the discretion of the owner who performs the policy defining and the specification of resources accessible by subjects is done by the owner. The distinction of subject and object is the basis to control access. DAC allows owners of the objects to propagate permissions to other subjects. Access request is initiated by the subjects. The access is granted or denied based on the identity of the user or group. When a system receives a request to access an object, the authorization mechanism checks the subject's identity and then grant access.

Access control lists are the most common implementation of DAC which are enforced on the operating system level and set by the owners. One of the drawbacks of this model is that it lacks centralized control. It provides a framework for resource protection in operating systems. Access control in systems like Linux, Unix, and Windows are based on discretionary access model. The rights possessed by each subject to access a certain object are depicted in the access matrix. For an access control matrix, A, rows represent the subject's ‘s' and column represents the object ‘o'. The access rights of a subject for the object are A [s, o].

The implementation of the access matrix can be done in multiple ways. It can be read by columns, rows or tables. The capability list of the user is determined by reading the matrix by rows. It determines the access rights for each user and mostly implemented in distributed systems. When it is read by columns the access matrix is interpreted as ACL which determines the permissions granted to a particular object. Centralized systems mostly use this type of method. The access matrix, when read by tables, is interpreted as access control triples. Such implementation is widely used in database systems. The table has subjects, access modes and objects specifying access rights of subjects over objects.

There are some limitations in the discretionary model, the complete control of a user on the access rights of an object creates issues. Due to the unrestricted ownership of access rights on objects, the verification of policies also becomes complicated. It is also susceptible to Trojan Horse where maliciously files can be copied. The absence of

restrictions on rights propagation and copying information increases the risk of malicious activities. Moreover, with a large number of subjects and objects, DAC model becomes more complicated.

2.2.2 Mandatory Access Control Model

The mandatory access control is a structured model based on the security labels that consist of classification and categories. The security clearance is given by classifying the subjects on different security levels as top secret, secret or confidential. Similarly, objects are also classified. The classification and clearance data are assigned to the objects and subjects. The need to know rules are enforced based on the categories. Access is granted on the basis of clearance of the subject, classification of the object and security policy of the system. Mandatory access control model is mostly used in systems where confidentiality and classification are most important such as the military. The implementation of MAC on Linux OS is Security Enhanced Linux.

2.2.3 Non-discretionary/ Role-based access control

Non-discretionary or role-based access control (RBAC) is based on user roles or groups with defined business objectives rather than individual identities. The interaction between objects and subjects is determined by the set of controls that are centrally administered. RBAC relies on the structure of role assignment, authorization, and permissions developed through role engineering to regulate access. Access control administration is simplified by the RBAC model, so it is best suited for companies that have high employee turnover and used widely in businesses (O'Connor & Loomis, 2010). This model can also be used in combination of MAC and DAC models by configuring roles.

Due to the flexibility and ease of administration, RBAC is extensively used in various applications as it can express a wide range of security policies. Oracle database and Windows Server 2003 have used RBAC for managing authorizations. The notion of RBAC was first proposed by Ferraiolo and Kuhn (1992) in the early 1990s. Later further research was conducted and a family of reference models for RBAC was defined for its applications in various systems. The role has been defined as a collection of permissions (Ferraiolo, Cugini, & Kuhn, 1995). These roles are then assigned to the users which as a result acquire the permission associated with a role. The access can be controlled by administrators by limiting the rights assigned to the role. This method is quite effective

for enforcing security policies and well-organized access control process. Due to its advantages, it was soon adopted in the field and was the most preferred model.

2.3 Access Control Techniques

The access control models define the policies from a high-level perspective whereas, access techniques are the enforcement mechanism that describes implementation architecture (Sandhu, Ferraiolo, & Kuhn, 2000). Different access control techniques are available to support access control models.

2.3.1 Rule-Based Access Control

This technique uses specific rules which specify the interaction between the subject and object. Access to object is not identity-based rather it is granted if the predefined rules are met by the subject irrespective of identity.

2.3.2 Constrained User Interface

The constrained user interfaces are used to restrict access of the user by limiting their access to specific resources or their ability to request particular information or functions. Database view, menus, and shells, and physically constrained interfaces are three main types of restricted interfaces.

2.3.3 Access Control Matrix

It is a table that consists of all objects and subjects that depicts the subjects of the permissible action can take on objects. Access rights are assigned to both subjects and objects known as capabilities and access control list respectively. A capability table is used in this technique to specify the capabilities of a subject with respect to an object. A capability could be in various forms such as key, token, and ticket. In the matrix, each row represents the capability and ACL are represented by the column for a specific user. Such a capability-based system is used in Kerberos where the user is provided with a ticket. Access control lists define subjects, objects they are authorized to access and the level of authorization at the individual and group level. The mapping of the values from the access control matrix to the object is done by ACL. The ACL is bound to an object, but the capability model is bound to a subject.

2.3.4 Content Dependent Access Control

The access is based on the content of the object such as email filtering, database views.

2.3.5 Context-Dependent Access Control

The context of a collection of information is the basis for access decision rather than sensitivity of information such as context-based access decisions are used in the firewall where state information is collected before allowing the packet into the network.

2.4 Access Control Planning

According to Hu et al. (2006) during the planning of an access control system, the three main abstractions that must be considered are policies, model and mechanism of access control. Access control policies define the high-level requirements which specify access management and which resources and information can be accessed by whom (Lampson, 1974). These can be application specific and thus taken into account by the application vendors but are relevant to user actions within the context of an organizational unit. For example, policies may concern the usage of organizational resources or based on various factors like need-to-know, authority, conflict of interest or competence.

The access control policies are enforced through some defined mechanism on a higher level that translates the access requests of users in terms of a system provided structure. There are various structures such as simple table lookup that can be used to translate the processes of granting or denying access. Due to the lack of a well-accepted standard, few access control mechanisms are actually direct implementations of the relevant access control policies.

The security properties of an access control system are specified by security models instead of evaluating and analyzing systems on mechanism levels. A security policy is formally represented by a model that is useful to depict the theoretical limitations of a system. Access control models bridge the gap in abstraction between access control policies and access control mechanisms. Access control mechanisms can be designed in a way that they comply with the properties of the models. As for the users, the model is a precise and clear expression of requirements. Whereas, for the system developers it represents the design and implementation requirements. Access control model could be either flexible enough to allow enforcement and expression of various policies or rigid in the implementation of a single policy. Moreover, access control policies can be changed over time due to ever-evolving regulations, business requirements or other factors.

Several well-known access control policies are classified as non-discretionary and discretionary. Where former is associated with rule-based and latter with identity-based access control.

2.5 Role-Based Access Control (RBAC)

In RBAC the access of users to information is regulated on the basis of functions performed by users. Identification of the roles in the system with role-based policies is important. A role is a set of permissions used to access appropriate resources as per job function. Instead of defining all authorized accesses for a user, authorized access to objects is specified for roles and users adopt those roles.

2.5.1 Role Based Access Control Models

Alan O'Connor and Ross Loomis (2010), have discussed different models of role-based access control. The RBAC model taxonomy consists of four models i.e. core, hierarchical, static constrained, and dynamically constrained RBAC. The basic RBAC system features are covered by Core RBAC. The concept of role hierarchy is defined by hierarchical RBAC that uses inheritance relation to define the partial ordering of roles. Constrained RBAC includes properties of dynamic and static separation of duties that are applicable on a session or all-time basis. Constraint relations that are imposed on role assignment relations are added by statically constrained RBAC. The dynamic constrained RBAC imposes the constraints on the activation of sets of roles that may be included as an attribute of a user's subjects. These models have been further discussed below.

2.5.1.1 Core

In the Core, role-based access control model permissions consist of operations applied to objects. The administrative sets in this model are roles, users, objects, operations, and permissions. Access policy is designed around role which is a semantic construct. Roles have associated permissions and users are members of roles, therefore, acquiring those permissions. A user can be associated with one or more roles. Similarly, a role can have one or several assigned users. This arrangement makes it flexible and allows granular assignment of permissions to roles and users to roles.

2.5.1.2 Hierarchical

Roles in the RBAC model can have overlapping privileges and responsibilities that means users associated with various roles required to perform common operations. Under RBAC, roles can have overlapping responsibilities and privileges; that is, users belonging to different roles may need to perform common operations. Similarly, some operations are general that are required to be performed by all employees. Specifying such general operations for every role would be cumbersome and inefficient thus establishing the role hierarchies to comply with the organizational structure.

Role hierarchy defines roles with unique attributes that may have other roles which imply that roles might contain operations that are also associated with another role. For instance, in a healthcare department, a single role of specialist could have the roles of Intern and Doctor. In this way, the members of Specialist role are inherently connected with associated operations of Intern and Doctor's role's without having to assign the Doctor and Intern operations.

Moreover, each of the roles of Rheumatologist and Cardiologist could contain the specialist role. This is a way to reflect responsibilities, authorities, and competencies. The role to which user is being assigned is not mutually exclusive with another role for which the user already possesses membership. These roles and operations are dependent on the constraints and policies of an organization if overlapping operations exist than such role hierarchies can be established.

2.5.1.3 Statically Constrained

Organizations can restrict access by implementing role-based access controls instead of appointing auditing companies to monitor access. For instance, access to patient records can be given to physicians if a sufficient access control process is in place. Constraints on the physician access can be set up with RBAC so that particular physician is only able to access those records that are authorized. Rules can be established by organizations to associate certain operations with a particular role. For example, the role of the clinician can be restricted to only post the patient's test results but not allowed to distribute them to avoid any breach to patient's privacy due to human error and routing. The associated operations with a role can be specified in a way that they demonstrate the enforcement of

certain laws and regulations such as the role of pharmacist can have associated operations to dispense but not authorized to prescribe or provide medication.

Complex security constraints or requirements can be captured in an operation that is difficult to be determined by a simple mode of access. Hence operations act as a unit of controls referenced by the particular role that is affected by the constraints in the RBAC framework. For instance, in a bank, the access needs of the role of a teller are different than those of an accounting supervisor. The teller role is defined to perform a savings deposit operation which requires the access to read and write specific fields to a savings file.
Similarly, the role of accounting supervisor can be defined to perform correction operations which require access to the same fields of saving files as the role of teller has. Nonetheless, here the constraints apply on the role of accounting supervisor that is only authorized to perform corrections but not initiating withdraws or deposits. In the same way, after the completion of the transaction, the teller cannot perform any corrections. The difference lies in the associated operations of two roles as a result of which they write different values to the transaction log file.

2.5.1.4 Dynamically Constrained

The role-based access control framework provides a framework for administrators to manage operations that a member of a role is authorized to perform. There could be a limit on assigning the users to a certain role at any given period of time. Such as only one employee can be assigned to the role of a manager at a time. In spite of some employee may act in the role, other than the manager but only one person is allowed to own the role at a given time. Memberships for roles can be assigned to users as long as it does not exceed the maximum number of users allowed for that role.

Users are able to carry out a wide range of legitimate operations due to the flexibility and broadness of application provided by a well-administered RBAC framework. Access can be controlled by the system administrators at the level of abstraction according to the business requirements of an organization. This is accomplished by managing user actions dynamically and statically through formulation and definition of roles, relationships, role hierarchies, and associated constraints.

Therefore, once the RBAC framework is in place, the major administrative task is removing or assigning a user to a role. This process is unlike the traditional and less intuitive processes of managing access on an object by object basis e.g. access control matrices and access control lists (ACL). RBAC also allows the association between the RBAC operations and "method" in object-oriented technology. This leads to the implementation of RBAC operation in operating systems and applications by using object-oriented technology.

RBAC is adaptable for a wide variety of organizations such as industrial or government organizations have varying security requirements. Despite that, only limited systems are commercially available that implemented RBAC. Oracle Enterprise Server, Informix Online Dynamic Server, and Sybase Adaptive Server are few popular commercial database management systems that support the implementation of basic RBAC features.

2.5.2 Role Based Access Control for Distributed Systems

A variety of enterprise management and resource providers offer additional administrative capabilities to manage the fundamental access control mechanisms of database management, hosts, network operating systems, applications, and file management. This leads to layers of access control management systems on the top of each other. However, few principles are based on the simple access control mechanisms that are supported by a single sign-on system and appropriate for environments with distributed systems. Hu et al. (2006) describes these principles as below.

- Grouping of users by roles
- Access rules
- Centralized control

These have been further discussed along with access control mechanisms.

2.5.2.1 User Grouping by Roles

An organization that has RBAC in place can centrally control its resources. This model is different than DAC, where the resource creator determines who is authorized to access it. In most of the organizations, although an employee could be the one creating the resource, the actual owner of the resource is an organization that wants some control over resource sharing.

The scalability and flexibility are greatly enhanced by RBAC which provides the delegation of administration and gives a certain level of control to a user. However, it may also reduce organizational control over resources. The responsibilities of administrator in RBAC distributed systems can be divided at central and local domains. In this way, the central security policies can be defined at the enterprise level and the local security issues can be left for the organizational unit level.

For instance, in a distributed healthcare system, those operations which are associated with healthcare providers and applicable to all clinics and hospitals may be specified centrally. However, the assigning and removing of users to specific roles may be specified by administrators at local sites. Apart from self-contained resource management products like operating systems and DBMSs, RBAC has been implemented also in Enterprise Security Management Systems ESMS. ESMS products are used for the centralized management of authorization of resource in the target systems that are distributed across the organization.

ESMS basically create and manage the mappings between the system level user accounts, groups and their membership with enterprise-level users, roles and their memberships. This is executed by the ESMS with the help of agent software running on each system, that creates and deletes user accounts and groups. Moreover, it also assigns user accounts to the groups. Further, assemble the access control lists based on the enterprise level commands received. The fundamental parts of the mapping of system level permissions to RBAC semantics at the enterprise level are the user's IDs and groups.
The mapping of an organizational view onto a system level group is done by assigning users to groups that are inherited by or assigned to its corresponding role. In such a technique instead of assigning permissions to roles, they are assigned to groups which are then mapped with roles organized into a role hierarchy. Due to this hierarchy, groups that are assigned to a role are mapped to all the higher roles in the hierarchy.

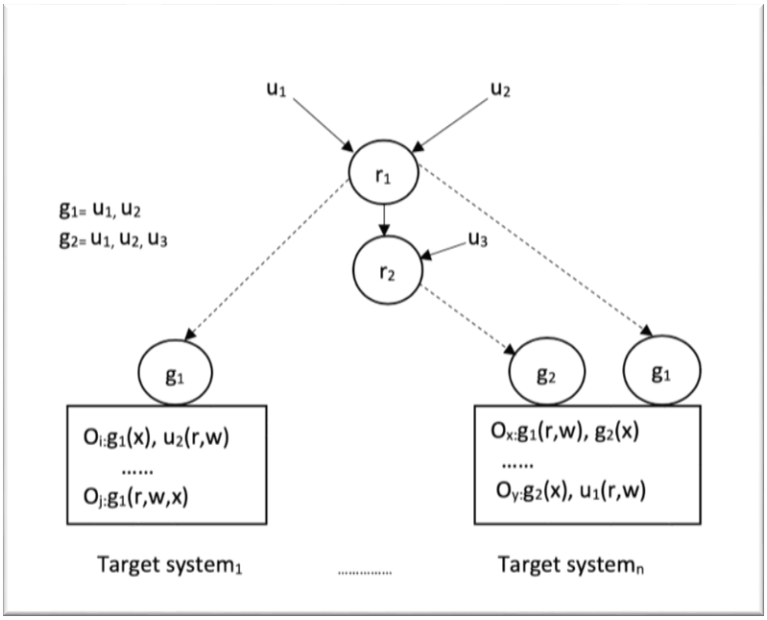

Figure 1.1. Mapping RBAC for Distributed Systems (Hu et al., 2006)

Figure 1.1 shows the links between the circled nodes representing the roles, groups, and assigned users shown as regular arrows, inherited non-circled users with heavy arrows and assigned user with regular arrows. The group-to-role relations are represented with dotted arrows so that if r_1 inherits r_2, a user that is assigned to role $r_1$also becomes a member of all groups mapped to role r_2 and also becomes part of role r_2.

Groups act like a bunch of permissions as the ACL for a particular target system which is shown in the blocked text with the format of an object: group (permitted operations), group (permitted operations) ...), apart from the inheritance of role and groups, permissions are also inherited. The membership to the local group is granted to a user by ESMS when an account in the system exists. Therefore, for any user to be associated with any group, the existence of the local system account is necessary.

On the basis of the subgraph concept, enterprise roles, user and mappings to groups and accounts can be initially created by ESMS. One of the more roles in the role hierarchy can define a subgraph. The defining roles and user or role that inherits the defining roles are included in the subgraph corresponding to the roles. As shown in the Figure 1.1 that the subgraph initiated by role r_1 is mapped onto Target system-1, whereas the subgraph defined by role r_2 is mapped onto Target system-2.

This mapping of role to group and user to the account can be performed over any number of target systems by ESMS. The enterprise-level deletion of the user's role assignment can result in the deletion of a user's membership in multiple groups in various systems. However, deleting a user on enterprise level results in deletion of all user group memberships and accounts in all target systems where the user existed.

Similarly, enterprise-level assigning of user role results in the creation of group memberships and accounts within all system for which the user assigned role was initiated. Such a scheme can be used in an RBAC system to manage user groups and IDs across the control domain by managing the user-role assigning and inheritance at the enterprise level. Once user IDs, group and memberships are created by ESMS at the system level, local resources can be protected by local users by expressing local permissions with the help of user IDs and groups.

In certain implementation, the user might belong to a single group and thus inherits only the attributes and operations associated with the group. However, in the case of conflicting settings, the group level settings are overridden by user level settings by default. Users who authenticate but are not mapped to an existing group, are assigned to the default group. As an alternative, the user might not be mapped to a particular group instead an external authenticator maps the group. The system can collect the group information from the external user database where the defined group memberships for the user can be associated with specific groups.

2.5.2.2 Access Rules

Any attribute of a system related to users can be used to establish role-based access control. These attributes could be host, domain, protocol, IP address or network. For instance, the user wants to access some object in another network on another side of the router. The user is granted or denied access based on the role-based access control and the rule based on network attributes. The existing authentication credentials are still valid if the change in role occurs within the organization and do not require to be reconfigured. When rules are used in combination with roles, flexibility is added as rules are applicable to both devices and people.

Applying the role-based access control in a distributed system requires to define the attributes used for rule constraints to avoid conflicts in rule set that can lead to leaking of privileges. Therefore, constructing rule-based algorithms is vital. For example, consider a quality engineer and product engineer which are two basic types of software users. Both groups have different roles in relation to data and functionality of application but can access the same data. Moreover, people in these groups have varying job responsibilities that can be identified by several attributes. The confusion is avoided by maintaining access to profile rules and application-specific position codes for a particular user. The data owner identifies attributes when storing data objects that express the purpose and content of the document. When the application is executed, access rights for the user are determined by matching the user profile and position codes with the attributes in the document.

Another way to make access decision based on the information in the directory could be using a person's role or set of rules based on user attributes. Such a system allows access to resources and information to be managed for individuals based on their roles or other associated factors such as department, office location, and language. For example, there could be a need to view a completely different set of web resources by two employees with different roles at different locations.

2.5.2.3 Centralized Control

Several organizations with distributed systems manage and store their data centrally. In such a scenario, access to the centrally stored data is managed by a centralized access control system. The central access system can also delegate the access controls to subsystems depending upon the organizational size and structure. They may also dedicate a server for this purpose which is independent of the business network of the organization. The commonly used techniques are Centralized Object Access and Delegation of Administration Privilege, a model that was designed originally to fit into distributed network and systems (Hu et al., 2006).

2.5.3 Role Engineering

Role-based access control has been implemented in a variety of commercially available system like banks and insurance companies (Ma & Li, 2010). Before the benefits of

RBAC can be achieved, the challenging task is to create a comprehensive framework where the architectural structure of RBAC can be defined. Role engineering is the process to migrate a system not based on RBAC to an RBAC system.

E.J. Coyne (1995) introduced the concept of role engineering in 1995, to define a complete, efficient and correct structure to specify the security policies as per the business functions. The two basic approaches for role engineering are top down and the bottom up. In the top-down approach, the business functions are analyzed, and roles are derived from them and then the needed permissions are assigned to roles. Although this approach is costly and time-consuming but reflects the actual organizational functional requirements. For medium to large size organizations, the top-down approach is impractical as they have thousands of users and a lot of business processes (Coyne, 1995).

Under the bottom-up approach, the existing user permission assignments can be used to aggregate roles automatically before the implementation of RBAC. Hence, the business functional requirements of an organization are most likely to ignore but it leads to the generation of the architectural structure of RBAC automatically. Researchers have focused on the application of data mining techniques in role extraction and defining (Frank, Buhman, & David, 2010).

When roles have the associated permissions and users are assigned to roles then users get the privilege required to perform their job. As various job categories can lead to the overlapping of responsibilities so giving the maximum privilege can lead to unauthorized access. Here the concept of least privilege plays its part in which users are assigned just the minimum privilege that is required to perform their job by identifying user's job functions and restricting the user to specific privileges only.

In systems that are not precisely controlled, it is difficult to adjust access based on several constraints and attributes making it costly and difficult to implement. In this case, the concept of role hierarchies can be utilized that sustains the natural structure of an enterprise. Roles are defined with unique attributes and one role may contain another role which means it includes the associated operations of another role.

2.5.4 Constraints in RBAC

The key challenge in the migration of a non-RBAC system to RBAC is the way constraints should be generated. Most of the existing approaches for role engineering use the business rules of organization and then reflect these in the defining, naming, constructing and structuring some valid set of roles. Constraints are an important part of RBAC, but no approach exists that use existing user permission assignments to mine constraints. For instance, in a bank purchasing manager and account payable manager are two mutually exclusive roles so the same individual will not be permitted to have both these roles as it can create a conflict of interest leading to fraud. Similarly, only one person can take the role of chairman of the department. In the same way, there could be a limit on the number of roles to which user can belong to. This is called cardinality constraint (Sandhu, Coyne, Feinstein & Youman, 1996).

The traditional approaches of role engineering only identify roles and place them into a role hierarchy, whereas the constraints are also important and most distinctive feature in RBAC. The set of imposed rules on RBAC are called constraints. The RBAC architectural structure is incomplete without constraints.

As the role-based access control system focuses on the access control to resources and operations and can support the principles of least privilege, separation of duties and data abstraction. For instance, there is a set RQ = $\{p_1, p_2, p_3, p_4\}$ which contains the requested permissions required by a normal user to perform tasks. The principle of least privilege can be applied to the requested permissions by the set of roles $\{r_1, r_2\}$ by covering all the permissions in the permission set. However, if the concept of constraints is not applied than the application of least privilege is not useful. For example, knowing that roles r_1 and r_2 are mutually exclusive or not is important.

Constraints provide a mechanism to lay out organizational policies on a higher level. The chief security officer can lay out what is acceptable in a broad scope and this is imposed a mandatory requirement for others participating in RBAC management i.e. users and security officers. In the absence of such a mechanism, the administrator cannot do this.

The components of RBAC model are users, roles and permissions represented as U,R,P respectively (Ma, Li, Lu, & Wang, 2011).

- PA ⊆ P × R, a many-to-many mapping of permission-to-role assignments;
- UA ⊆ U × R, a many-to-many user to role assignment relationships;
- auth_perms(R) = {p ∈ P |(p, R) ∈ PA}, the mapping of role R onto a set of permissions.

Before the RBAC implementation, an m x n binary Matrix can be used to describe users and permissions relationship, where m and n represent the number of user and permissions respectively. The element M{i,j} = 1 represents the i_{th} user has the j^{th} permission or vice versa. u_i (i = 1, . . ., m) indicates the i_{th} user and its associated permissions. $(u_i)(i=1,...,m)$ indicates the set of permissions assigned to the i^{th} user. p_j (j=1,...,n) indicates the j_{th} permission and users with those permissions. (p_j) (j = 1, . . . , n) indicates the users that have permissions P_j.

When role engineering is used in RBAC, the m x k binary matrix to describe user and role relationship, where m represents the number of users and K($k \leq n$) indicates the number of roles. The element N{i,j} = 1 denotes that the i_{th} user has the j_{th} role or vice versa. u_i (i = 1,...,m) indicate the users and their roles, $(u_i)(i=1,...,m)$ indicate roles assigned to i_{th} user, r_j (j=1,...,k) indicate the j_{th} role and role_users (r_j) (j = 1, . . . , k) to indicate the set of users that possess role r_j. Therefore, various constraints have been discussed by Ma et al. (2011) as follows.

Mutually exclusive roles: Given a set of roles $r_s \subseteq R$, then $r_i \in r_s$ and $r_j \in rs$ ($i \neq j$) are mutually exclusive roles, if role_users(r_i) ∩ role_users(r_j) = ∅. The constraint specifies that an individual cannot be a member of both roles that are mutually exclusive. We can also say that a user can be assigned to one of these roles at a time. For instance, the user can have one of the account managers and purchasing manager roles at a time but not both. If we represent $r_i \wedge r_j$ as r_i and r_j as mutually exclusive roles than if we have two roles set $\{r_1, r_2\}$ and $\{r_3, r_4\}$ then the user cannot be part of both.

Mutually exclusive permissions: Given a set of permissions ps ⊆ P, we say $p_i \in p_s$ and $p_j \in$ ps are mutually exclusive permissions if $p_i \in$ auth_perms(r_i), and $p_j \notin$ auth_perms(r_i) for all $r_i \in R$. If we represent the mutually exclusive permissions by pi and pj then both permissions cannot be assigned to the same role. For instance, the permissions to audit

operations and issue checks should not be assigned to the same role. Hence if we have permission sets that are mutually exclusive $p_1p_2 \wedge p_3p_4$, the role cannot be part of $\{p_1, p_2\}$ and $\{p_3, p_4\}$ or $\{ p_1, p_2\}$ and $\{p_3, p_4\}$.

Cardinality constraint of the role: It is defined as a maximum number of roles to which a single user can be associated. As the principle of least privilege is one of the most important principles in RBAC which states that user should be able to access resources needed to complete the regular tasks. If the requested permission set is represented as RQ = $\{p_1,p_2,p_3,p_4,p_5,p_6\}$, and authorized permissions by auth_perms $(r_1) = \{ p_1,p_2,p_3\}$, auth_perms$(r_2) = \{p_3 , p_4 \}$ and auth_perms$(r_3) = \{ p_5,p_6\}$. Then the principle of least privilege can be enforced by role set $\{r_1 , r_2 , r_3 \}$ for the permission set RQ if the constraint on the maximum number of roles a user can belong to doesn't exist. However, if each user cannot have more than two roles, then no role set can satisfy the principle of least privilege for the requested permission set.

Cardinality Constraint of User: This defines the maximum number of users that a role can have such a department can have only one chairman. So, no two users can be assigned to this role at a time.

Cardinality Constraint of Permission: This constraint defines the maximum number of roles to which permission can be assigned. For example, in the case of database transactions, certain permissions can be only assigned to a limited number of roles to avoid conflict.

2.5.5 Temporal constraints in RBAC

Several applications require temporal constraints. These are the formal statements of access policies that involve access restrictions to a resource based on time. In some applications, resource use can be limited by temporal constraints. Whereas, others may require it to control activities that are time sensitive.

In addition to other constraints, such time-based constraints must be evaluated for dynamic authorizations generation while the execution of the workflow. Such a constraint may be required for non-workflow environments for instance, in a banking enterprise, the role of a teller should be assumed by an employee who performs transactions on customer

accounts during specific timings. To execute this, temporal constraints are required that can limit the availability and activation of role only to designated banking hours.

History-based access control policies are among the few known access control policies related to temporal constraints that have practical application in various business activities like separation of conflicts-of-interests and task transactions.

2.5.6 Least Privilege

Nwafor and Zavarsky (2012) have discussed the principle of least privilege. In the role-based access control model, set of permissions are assigned to roles which are associated with users. The complexity of access control is reduced when access permissions are assigned in this way as the number of users is much larger than roles in an organization. Moreover, one of the three well-known security principles that are supported by RBAC is the least privilege.

The principle of least privilege is one of the most important principles in the designing of security policies. When feasible, users should be granted the minimum level of access to complete a job function. We can also say that the system should be able to determine for a particular user the least privilege to perform the task and ensures that no more than the required privilege is granted.

2.5.7 Separation of Duty

Separation of duties also known as segregation of duties minimizes the potential to abuse the authorized privilege rights and reduces the risks of malicious activities (NIST, 2014). It ensures that no individual should have the authority to complete multiple conflicting tasks. It is one of the basic internal controls and the idea is to assign the privilege to complete a critical task among several individuals. The concept of separation of duties is well-known in the financial systems since long ago. However, this has also become relevant in the IT industry and greater emphasis has been given to it lately.

The primary objective of SoD is firstly to prevent conflict of interest, fraud, abuse, and malicious actions. Secondly, the detection of failure of controls such as information theft, security breaches and circumvention of security controls. The designing of separation of

duties should be done in such a way that no individual should have conflicting responsibilities. There are two main types of separation of duties.

2.5.7.1 Static Separation of Duty (SSOD)

In the static separation of duties, conflicting roles are specified by the predefined set of rules. It prevents from assigning conflicting roles to system users which minimize the risk of conducting fraudulent activities. With the increase of individuals involved in the execution of a critical task, the chance for any malicious activity to take place is reduced.

2.5.7.2 Dynamic Separation of Duty (DSOD)

In the dynamic separation of duty, the separation of duty is enforced at the time of access. The user can be assigned multiple conflicting roles but only a single role is activated at a time to perform the relevant job functions.

2.5.8 Limitation of Role Based Access Control

Hu et al., (2006) discusses the limitations of the RBAC model. As it works by assigning permissions to roles which are further assigned to the user. So, encapsulating all the permissions for a role required to perform a job is necessary. The first step to implement RBAC is role engineering. When roles are constructed, the most challenging part is to decide between ease administration or strong security.

In the easier administration, roles with similar permissions can be merged into one role. Thus, reducing the number of roles and also making the management easier. However, if stronger security is the preference here then each and every role should be more granular and well defined. This can also lead to assigning multiple roles to a single user (Kuhn, Coyne, & Weli, 2010). An organization should be able to find some balance between two approaches.

With the technology becoming more and more incorporated in businesses leading to an increase in the number of applications and systems. Moreover, the development of cloud technology is making the technological structure of organizations more complex. In such a scenario, RBAC alone cannot fulfill the access control needs of a company with a complex structure. Therefore, it should be combined with other access methods such as Rule-based access control to achieve more practical value (Hu et al., 2006).

The implementation of segregation of duty is another limitation of RBAC as it requires careful role designing and assigning them privileges. In the process of assigning privileges, it should be ensured that the existing segregation of duty control is not affected by assigning new privileges.

2.6 Related Terms in Access Process

Some terms that are used in the access control process are worth mentioning here as they will be used in explaining the process workflows (Kissel, 2013).

Owner entity or person who has been approved by management for the responsibility of controlling the development, production, maintenance, security, and usage of the asset.

Requester Person who submits the access request with the required information.

Approver Person who reviews the access request according to policies and procedures.

User Individual who uses the IT service. Users can be different from requesters and customer as some of them may not use the service directly.

Service Owner Entity responsible for managing the service throughout its lifecycle.

Service desk the point of contact between the user and the service provider.

Escalation additional resources obtained by activity when needed to meet customer expectations and service level targets.

Change The modification, addition or removal of anything that affects the IT services.

Event occurrence of a change of state that effects the management or configuration of IT services.

Incident An unplanned interruption to an IT services or reduction in the quality of the service.

Closed The final status in the lifecycle of a change or incident. No further action can be taken once the status is closed.

Service Desk The single point of contact between the service provider and the user.

2.7 Security Standards

The information security standards SOC 2 and ISO 27001 provide the best practices to implement security controls for businesses. By complying with these standards an assurance of trustworthiness of business is provided by an organization to the customers.

2.7.1 ISO 27001

An access control system to be compliant with ISO 27001, there is a need to have a processor solution that is in line with the defined criteria. If concerns regarding data leakage, malicious attacks and hacks are raised by clients, an organization that is compliant with ISO 27001 is able to show the process and controls in place. Companies can implement the ISO 27001 compliance in parts by choosing the division that needs to be certified and establishing the processes and controls for that area. Client satisfaction, legal harmonization, and financial returns are the major benefits provided by ISO 27001 (ISO/IEC-27001, 2013).

2.7.2 SOC 2

The SOC 2 compliance report is associated with security mechanisms and procedures. The compliance report has three basic reports i.e. SOC 1, SOC 2, and SOC 3 that an organization can achieve. Further, the compliance is governed by five fundamental attributes provided by Trust Service Principles i.e. security, privacy, confidentiality, availability, and processing integrity. Among these, the SOC 2 access control is compliance is directly governed by security principles.

Both logical and physical access should be restricted to complete access protection. The access procedures for the data, assets, and resources should be designed properly according to the rules and regulations. The access should be authorized, based on the ID and easily traceable. The personal information should be both logically and physically protected. Moreover, the collection, usage, storage and disposal of data should be as per privacy policy.

Further, the confidentiality should be maintained as agreed with the customers, users, and stakeholders of the company. Similarly, processing integrity and availability should be compliant with the agreements and standard policies. The compliance with some of the

rules specified above qualifies an organization as SOC 2 access compliant (AICPA, 2018).

2.7.3 Purpose of Access Compliance

Complying with the standards means following the laws and standards. In the context of access control and security, it means having a standard of the way of granting access, managing and storing permissions. A compliance certificate is a document issued by the authorities which provides the surety that a product or service meets the necessary specification to be used. When it comes to the security of access control systems, compliance certification accounts for quality regarding safety, usability, and efficiency. Complying with a reliable certification authority ensures the overall functionality of a physical access control system.

The objective of access control is to limit access to information and services to limited people based on a certain criterion. It is ensured by the certification that services provided by the security system abide by the established rules and processes. With the world becoming digitized, malware and hacks are also increasing. An access control system that is compliant ensures that the system is capable of resisting malicious attacks. Apart from restricting the access, the access control system should also make sure that the files are secure and accessible. Compliance certification ensures the quality and accessibility of the access control system.

For organizations dealing with customer data, having their access control process certified with a regulatory body like SOC or ISO plays a vital role in their business. It not only acts as a symbol of quality for a service or product but helps in sustaining over time. Moreover, certification helps in designing more organized and reliable processes. In addition to that, a compliance certificate improves the credibility and reputation of organization which leads to an increase in the organizational revenue due to consistent performance and customer satisfaction.

Chapter 3

3 Systems and Requirements

This chapter discusses the systems that are involved in the access management process directly or indirectly. There could be other available systems that are better, but these systems were preferred by the organization due to their availability in the organization. All these systems are being used already either in the access or user management or some other processes.

3.1 System Context

3.1.1 Customer Environments

The organization provides SaaS solutions to retail businesses. The single tenant SaaS architecture allows for a single instance of software to run for each customer on SaaS servers. Some customers use the standard solution whereas most of the customers have their own specific requirements as per their business needs. To cater to this, the solution is customized according to customer requirements. These software instances running on cloud-based servers are called customer environments. The customer environments contain customer specific data that is used in the SaaS solution. This is confidential data that must be protected through processes and policies in place. Before the new access control process, it was a small organization where persons across the company were involved in working on multiple customer projects which required accessing several customer environments at one time. Therefore, there was no requirement to have access restriction to customer environments on a granular level. Moreover, the process to request, approve, log and track access was not following standardized security framework best practices. The organization is growing a lot and the new access control process has been implemented to align with the needs of growing organization.

3.1.2 Internal Systems

An organization is a collection of people, processes and systems which integrate to achieve a goal. The internal systems include all the applications and tools that allow an organization to run smoothly. These systems add all kinds of value for business and help the company to operate. The organization has various internal systems that vary from

project management to logging and tracking systems. Some of the systems are very essential for all employees to work and communicate effectively, others are just needed for certain teams and essential for their tasks. Similarly, varying access levels and permissions exist in the systems. Access to internal systems and privilege rights were not fully restricted. There was no process to log the provision and removal of access.

3.1.3 Identity and Access Management System (IAMS)

The identity management system which is used to manage the access of employees to organizational applications and devices. It is a cloud-based system which is compatible and integrates well with on-premises applications, identity management systems, and directories. The authentication for systems with customer data and other internal tools is done using the identity management system. This system will be mostly denoted as IAMS in the document.

Single Sign-on

Single sign-on is a way to manage multiple user accounts securely without affecting the integrity of individual applications. In order to get access to multiple applications, users can use one name and password. In this way, there is no need to log in separately to each application rather user login to the identity management system and gain access to all their applications. This capability saves users from remembering the credentials and the credentials are also safe. Single sign-on gives control over the applications by allowing tighter security and monitoring capabilities to ensure compliance with organizational policies and users are not making it more vulnerable.

Multi-factor Authentication

As the threats are increasing, the methods for authentication are also evolving. Multifactor authentication is used for increased assurance for web and mobile application. The process of authentication involves the validation of one of the factors like password, some identity or biometric methods like fingerprints. Multi-factor authentication uses two or more of these factors. The two commonly used factors by web and mobile applications for multi-factor authentication are password and time-based tokens. Moreover, MFA provides a way to application developers to increase the security of application access.

The system provides an identity management approach that facilitates business to take control of user identity and multifactor authentication to reduce data breaches. The customer data can be accessed via the identity management system which provides a centralized identity for users and reduces account management complexity. Access to applications can be restricted by intelligent SAML connections. As the user accesses all application via this service, audit trail for user actions and access in systems containing customer data are available. Logs can help in identifying any suspicious or unusual behavior.

User Access Management

Users and their associated attributes from applications can be stored in the universal directory. It supports multiple types of attributes including predefined lists, sensitive attributes, and linked objects. Users and groups can be created and managed, also permissions can be assigned based on attributes. Using the attribute-based policies, the access of the user to applications can be controlled using SAML and OAuth protocols. Once the user is authenticated, the system needs to understand if the user is authorized to access or interact with some application.

Role-based access control to applications

The identity management system allows to establish and maintain authorization policies that are based on the user context such as user profile and group membership. The access restrictions can be implemented by user types and permissions for which role-based access control can be employed. For instance, an IT person who will handle the IT admin tasks has the rights to create, delete and assign users to their relevant departments and teams. Similarly, product managers, developers, and architects have a different kind of privileges in a system. The varying responsibilities and policies are needed to be set in every group of the organization.

The RBAC model can be used to determine user permissions in a system as it allows you to apply granular and broad access policies. Different roles and their functions can be defined, and the user can be associated with some combination of roles. This approach also provides a logical model for auditing access which reflects an access structure and responsibilities.

3.1.4 Human Resource Management System

The HR Management System is used to manage personnel and their associated information. It maintains an organizational structure which contains all divisions, departments, teams, and sub-teams. The user data is kept up-to-date as it is the source system that provides the user attributes information such as title, role, and team. The user information is pushed from the HR Management System to other systems which need to maintain user profiles for process management. The change management process exists that enables updating the system as soon as user notifies about the change. Further, the changes are communicated to other teams managing their systems or pushed to those systems that are integrated with the HR Management System.

3.1.5 Jira-Ticketing and Logging System

Jira is a platform on which applications and products can be built to plan, manage and track project. It allows for creating different projects based on organizational requirements. There is three standalone product of Jira which can be used based on the requirements i.e. Jira core, Jira Software, and Jira Service Desk. The Jira Core is the basic project and task management solution whereas the Jira software and Service Desk are Jira applications that run on the top of it. There are multiple components of Jira which are described below (Atlassian, 2019).

Issues

Jira issues are work items of any size and type which are tracked from creation to completion. For instance, an issue could be a request to access certain customer data, development of a feature by the software team or a customer incident to be managed by the support team. The term mostly used for issues are tickets, requests or tasks.

Projects

A project is a collection of issues that are common in context. The issues in a project can be configured in several ways such as restricting visibility to workflows. Project is quite flexible as issues can be grouped by team, product, business unit or stream work. All issues grouped together in a project are represented by an issue key which is specific to a project along with issue number such as ACM-15.

Workflows

Workflows in Jira represent all the sequential steps that an issue takes from the point of creation to completion. A possible basic workflow is represented in Figure 3.1.

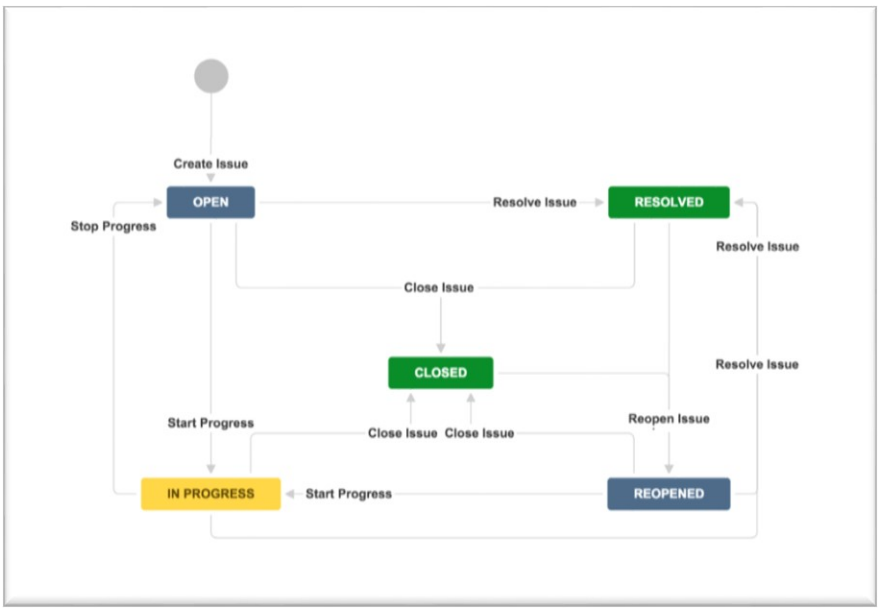

Figure 3.1. Basic Jira workflow

Workflows have a status such as open, done and transitions are represented by arrows from one status to another. Workflows can be of varying complexity with triggers, conditions, validators and post functions. The complexity of workflow depends on the business and project requirements.

3.2 Security Standards Requirements for Access Control

The access process was formulated as per the requirements from the security standards. Security standards were used as a criterion as they provide guidelines according to the industry best practices which have all sorts of value for the organization. ISO 27001 and SOC are the two main security standards that have been considered as these are well accepted in industries located in most of the parts of the world and the organization is aiming at certification. Further, the requirements provided by these standards for access control have been discussed.

3.2.1 ISO 27001 Access control

The objective of the access control is that the access to information, systems processing, and business processes should be controlled according to the organizational and security requirements. Access rights allocation procedures to services and information systems should be in place. These procedures should cover various stages of user access lifecycle. Moreover, special attention should be given to privilege access rights which give user higher level access to the system. Below we discuss the controls (ISO/IEC-27001, 2013) that are required and some guidance regarding their implementation (ISO-27002, 2013).

3.2.1.1 Access control policy

Control

An organization should have an access control policy in place. It should be documented and reviewed according to the organizational business and security requirements for access (ISO A.9.1.1).

Implementation guidance

The access control rules and rights should be stated in the access control policy for each user or user group. Both logical and physical access controls should be taken into account. In addition to that service providers and users should be given a clear statement regarding the business requirements that have to be met by access control. The access control policy as per the ISO 27002 implementation guideline should take following into account.

- The security requirements of business applications
- Information that business applications contain and their associated risks.
- The information authorization and dissemination policies such as the need to know principles, information classification, and different security levels.
- The information classification and access control policies should be consistent for network and different systems.
- Contractual obligations and legislation of an organization regarding access to data and services.
- Standard access profiles for users based on different roles in the organization.
- Access rights management in a networked and distributed environment.

- Access control roles segregation such as access request, access administration and access authorization.
- Access request formal authorization requirements
- Access control periodic review requirements
- Procedure for removal of access rights
- Differentiating between the rules to be enforced always and others which are conditional or optional.
- Rules should be established more in a stronger way that everything is forbidden generally unless allowed than the rule everything is permitted unless forbidden which is a weaker rule.
- Changes in information labels and user permissions that are automatically initiated by processing facilities and others initiated at the discretion of an administrator or user.
- Specification of rules that require approval and those which don't.
- The access control rules should have clearly defined responsibilities and supported by formal procedures.

3.2.1.2 User access management

User Registration and De-registration

Control

The formal user registration and de-registration procedure for granting and revoking of access to all services and information systems should be in place (ISO A.9.2.1).

Implementation guidance

The access control procedure for user registration and de-registration should include:

- User IDs should be used for individual identification of each user and to track their actions. Moreover, the use of group IDs should be permitted as per the business or operational requirements, but they should be approved and documented.
- System owner should authorize the user for the use of service and approval process for access rights management should be in place.

- The level of access rights granted to each user should be appropriate to business requirements and consistent with the security policy of organization such as segregation of duties should be maintained.
- A written statement of access rights for users, requiring them to sign and understand the access conditions by including a clause in personal and service contracts.
- Service providers should not provide access until the authorization process is complete.
- Maintaining a record of authorized people to use services.
- Managing the access rights based on the change of roles or change of employment.
- Periodic review and removal of redundant accounts and user IDS
- User access roles should be based on organizational requirements that compile access rights into user access profiles. The access requests and review of access rights are easier to be managed on the level of roles.

3.2.1.3 User Access Provisioning

Control

For all user and system, the assigning and revoking of access rights should be done through a user access provisioning process (ISO A.9.2.2).

Implementation guidance

The process or assigning or revoking access should include

- System owner should authorize users for the use of service or information systems. Process for access rights approval from the management can be also be in place.
- Verification of level of access rights assigned should be according to access policy and other requirements for instance segregation of duties.
- Access rights are only provided after the completion of authorization process.
- Central record is maintained regarding the access rights granted to users for accessing services and systems.
- Procedures for managing the access rights as a result of change of role or job and removal or blocking of access rights due to termination of employment.

- Periodic review of user access rights with system owners.

3.2.1.4 Privilege management

Control

The allocation and use of privilege rights should be restricted (ISO A.9.2.3).

Implementation guidance

System and services used by multiple users that require protection against unauthorized access should have the formal authorization procedures for allocation of privilege rights. The following steps should be considered:

- The access privileges regarding each system such as database management system, operating system, applications, and authorized users to have these rights should be identified.
- The privileged access should be allocated on the need to know and event basis as per the access policy.
- An authorization and logging process for privileged access should be in place.
- In order to avoid the need of granting privilege access rights, it should be encouraged to develop and use system routines.

3.2.1.5 Review of User Access Rights

Control

The formal process to review the access rights of users at regular intervals should be in place. To maintain effective control over information services and data access, regular review of access rights is necessary (ISO A.9.2.5).

Implementation guidance

ISO 27002 provides the following guidelines for the review of access rights.

- There should be a review of user access rights at regular intervals and after any change for instance demotion, promotion, and termination of employment.
- Review and allocation of access rights should be done when a change of employment occurs within the organization such as change of team.

- The privilege access rights authorization should be reviewed more frequently to ensure no unauthorized privileges have been granted.
- Changes should be logged for periodic review.

3.2.1.6 Removal and Adjustment of Access Rights

Control

The access rights of employees and external users to systems and services are adjusted upon change or removed upon termination of contract, employment or agreement (ISO A.9.2.6).

Implementation guidance

The access rights to information systems and services should be removed or reduced depending upon the evaluation of following risk factors.

- The change or termination is initiated by the management, employee or external party.
- Reason for termination
- The current responsibilities of the user.
- The value of assets that user can access.

3.2.2 SOC 2 Access Control Requirements

The SOC 2 compliance report meets the needs of a broad range of customer and users who need assurance about the organizational controls that affect the availability, security or processing integrity of services and system used by the organization to process data. SOC 2 reports can include one to five of the principles of Trust Services these are (AICPA, 2017)

- Security
- Availability
- Confidentiality
- Privacy
- Processing Integrity

3.2.2.1 Logical and Physical Access Control

Only the relevant clause from the logical and physical access control Trust Services criteria are mentioned below (AICPA, 2018).

- Restricts Logical Access— Logical access to information assets including software, hardware, authorities, output, administrative, data (at rest, transmission and processing), offline system components are restricted by access control rules and software.
- Identifies and Authenticates Users—the identification and authentication of persons, software and infrastructure is done locally or remotely prior to accessing information assets
- Manages Points of Access— Identifying, managing and tracking the points of access by outside entities and the data types that flow through them. The different types of systems and individuals that are using access points are identified, managed and documented.
- Restricts Access to Information Assets— Information assets access control rules are established by data classification combinations, port restrictions, separate data structures, access protocol restrictions and digital certificates and user identification.
- Manages Identification and Authentication— For systems and individuals that access entity information, requirements are documented and managed for identification and authentication.
- Manages Credentials for Infrastructure and Software— External and internal new infrastructure and software are registered, documented and authorized before implemented on the network or access point and access credentials are granted. When the access is not needed anymore, or the software and infrastructure are not being used then access is disabled and relevant credentials are removed.
- Controls Access Credentials to Protected Assets— The system owner or authorized custodian give authorization for the creation of credentials for information asset.
- Removes Access to Protected Assets When Appropriate— Establish procedures to remove access and credentials when a user no longer needs access.

- Reviews Appropriateness of Access Credentials— Periodically review of the appropriateness of access credentials is done to identify inappropriate users with credentials.
- Creates or Modifies Access to Protected Information Assets— Processes for access creation and modification of protected information assets based on asset owner authorization are in place.
- Removes Access to Protected Information Assets— Processes for access removal when no longer needed by the user for protected information assets are in place.
- Uses Role-Based Access Controls— Segregation of incompatible functions is ensured through role-based access control.
- Restricts Access— Restriction for the types of activities that can take places through a communication channel such as router port or FTP site, is in place.
- Protects Identification and Authentication Credentials—Mechanisms for protection of identification and authentication credentials during transmission are in place.
- Requires Additional Authentication or Credentials— When users access systems from outside its boundaries then additional credentials or authentication information are required.
- Implements Boundary Protection Systems— To protect external access points from unauthorized access, boundary protection systems (such as, firewalls, demilitarized zones, and intrusion detection systems) are implemented.

Chapter 4

4 Access Management Process Designing

Access management is the process of granting access rights to authorized users for using the service while preventing unauthorized users from accessing it. This process is referred to as identity and access rights management or access control process (ITIL, 2011). This chapter first discusses the purpose and objectives of the access management process and then it defines the scope for this process. Further it discusses the value that a business can get by having such a process in place. Moreover, after mentioning some related policies and principles, the designing of access management is discussed in detail.

4.1 Purpose and objectives

4.1.1 Purpose

The purpose of access management is to provide access rights for users so that they can use a service or some group of services. It involves the execution of information security policies and actions.

4.1.2 Objectives

The objective of the access management process is:

- The access management of services based on information security policies.
- Making the access management process efficient so that requests for granting, changing or restricting access rights are properly managed.
- Monitoring and logging the access to services and to ensure that the access rights are not being misused.

4.2 Scope

The effective execution of information security policies enables an organization to manage the confidentiality, integrity, and availability of its intellectual property and data is access management. Access management also ensures that users have the access rights to service as per the requirement or need but not at all available times. The process is mostly not separate rather all application and technical functions execute it. Nevertheless, there is always a single control point such as IT management or service desk for

coordination. The scope of the access management process is customer environments and internal systems of the organization. These systems have been described in chapter 3 where we have discussed their purpose and type of data they contain. The access process will be designed particularly for these systems.

4.3 Value to business

By implementing the access management process an organization can add value to its business in the following ways.

- An efficient and controlled access management process in place enables the organization to maintain the confidentiality of information.
- It ensures that employees have the right level of access to effectively perform their job.
- It reduces the human error in critical services by allowing only the user with the right skill set and rights to make changes.
- It logs the access activities which help in auditing and tracking the abuse of services.
- It provides the timely access to revoking capabilities which is important in case of critical security scenarios.
- It provides and demonstrates the compliance with security standards which help in ensuring the clients that their data is in safe hands.

4.4 Policies, principles and basic concepts

4.4.1 Policies

Access management policy for the organization includes the following aspects.

- The administration and activities associated with access management are guided by the controls and policies in organizational information security policy.
- The access management process involves the requesting, approving, granting and removal of access to services. Roles and responsibilities concerning the process have been defined.
- Access management process is able to log and track access activities and ensures that the appropriate level of rights is granted to users of services. This involves

appropriate processes for logging and tracking in place that can identify events regarding unauthorized access and misuse of access rights.

- The access management process is aligned in a way that changes in the personal events for instance change of role, transfer or termination of employment should lead to the adjustment of access rights accordingly. This involves a process in place that timely updates the changes that affect the access rights.
- Access management process maintains the access history to help in forensics and auditing activities. This involves a process in place that is maintaining the records with details such as who required access, level of rights requested, the reason for access and who granted the access.
- Procedures for handling, escalating and communicating security events related to access management have been defined and documented as per the information security policy. Those responsible for handling these activities are familiar enough with the policies and procedures in place to handle such events effectively and timely.

4.4.2 Principles and Basic Concepts

Access management process allows users to use services in the service catalog. This includes the following concepts:

- Access: the extent to which a user can use the functionality of a service or data.
- Identity of users refers to their information that distinguishes them and verifies the status of the user in organizations and identify them uniquely.
- Access rights or privileges: refer to the settings in the system that provide user access to services such as read, write, delete, execute, change.
- Service groups: Most of the users use multiple services and users who are performing a similar set of activities require access to a similar set of services. To make the process efficient, instead of assigning the rights separately to individual users, group of users is assigned the rights to set of services they are authorized to use at the same time.
- Directory services: refer to tools that are used in access management.

4.5 Roles in Access Management process

The roles, their responsibilities and which actor or system they related to in the access control process are defined in the below table.

Role	Responsibility	Actor/system
System Owner	entity or person who has been approved by management for the responsibility of controlling development, production, maintenance, security, and usage of the asset.	Service Managers for customer environments. Internal systems have their assigned system owners.
User	Individual who uses the IT service. Users can be different from requesters and customer as some of them may not use the service directly.	Jira Users
Requester	The person who submits the access request with the required information.	The employee requesting access in Jira
Approver	The person who reviews the access request according to policies and procedures.	Service Manager/Project Manager for customer environments. Internal IT for Internal systems managed by them. Specified approvers for other systems.
Service Desk	The single point of contact between the service provider and the user.	Jira Service Desk
Service Desk Agent	The person responsible for managing the service desk project	Support for customer environments access requests Internal IT for internal system requests HR team for change of status requests

Table 4.1 Role and responsibilities in access control process

4.6 Process Activities and Methods

The access control process is based on the role-based access model. There are two types of systems in our scope based on the information they contain i.e. customer and internal systems. The process has been designed with the requirements by security standards as the basis. The access to both types of systems has been designed through a role-based access control model so that the user is only able to access that is required to perform the job as per their role. The FLAT RBAC model has been used as it is the most suitable

RBAC model as per the organizational needs. It provides the following functional capabilities (Sandhu et al., 2000).

- Users require permissions through roles
- Supports many-to-many user-role assignment
- Supports many-to-many permission-role assignment
- Supports user-role assignment review
- Users are able to simultaneously use permissions of multiple roles

The principles of least privilege and segregation of duties are also implemented where required through RBAC (Ma; Ruixuan;Zhengding;Jianfeng;& Dong, 2011). Moreover, some controls have also been designed on the basis of "need to know" principle (NIST, 2013). The processes for both customer and Internal systems have been formulated in a way that there are not a lot of variations. However, there is a small difference in the processes as they have a different kind of data and users. Therefore, the processes have been explained for both systems separately and each process defines the activities for request, verification, granting and removal of access rights particular to that system. Jira is the ticketing and logging tool that has been used for access management process. All the processes that are discussed below have been designed in Jira.

4.6.1 Customer Environments

These are systems which contain customer data that is sensitive and need to have restricted access. The access to these systems is of two different types depending upon the urgency of the task, time period for which access is needed and most importantly the role (Loomis & O'Connor, 2010). Users are granted the access to customer environments as per the principle of least privilege i.e. only the minimum level of access or privilege rights are assigned to users while granting access (ISO/IEC-27001, 2013). A higher level of privilege rights has to be requested separately.

4.6.1.1 Permanent Access

The permanent access rights to customer environments are assigned to the group of roles that are working on the customer project. As working on the specific customer project is part of a role's responsibilities so according to the RBAC model they have the access rights to that particular environment. Apart from the project team, other users can also

request permanent access if needed by providing a valid reason. Users apart from project team can require access when they are working on a specific project task for that customer. The permanent access once granted lasts as long as the access rights are not removed by creating the removal of access ticket in Jira.

Granting Access

As Jira is being used to manage and log all access requests, the permanent access can be requested through Jira ticketing system. The process of granting access is as follows:

1. The requester will create a ticket by providing the following information.
   - Name/ name of the person on behalf of raising a request
   - Customer name
   - Reason for access
   - Description (optional)
2. The status of ticket will be OPEN, and the user will get a notification that access request has been created successfully.
3. The ticket goes into IN PROGRESS state and if the JSD agent needs further information from the user such as the reason for access is not clear, then comments can be added to ask the user for further information.
4. The Service Manager is the system owner for customer environments, so all access requests are approved by the Service Manager. Therefore, the approver is notified about the request.
5. The approver can assess the validity of request if valid then request can be approved else rejected.
6. The rejected requests will go to RESOLVED status and then automatically closed after some period of time.
7. If the request is approved, then access is granted to the user.
8. The status is changed to RESOLVED and user gets the notification that access has been granted to the particular customer environments.
9. When the ticket is in the RESOLVED state, there is a possibility to reopen the ticket. In the first case where access was approved, granted and resolved but the user is still not able to access so reopening is required. When the ticket is reopened it goes directly to the approved state.

10. In the rejected case, the reopening of the ticket might be required in case it was rejected mistakenly or due to some other reason. When the ticket is reopened after rejected and resolved state, it goes to INPROGRESS as it needs to go through the whole process again. The purpose here is that the user doesn't need to create a new ticket for the same request but just requests to reopen it.
11. Jira ticket can be canceled at any stage of the process.

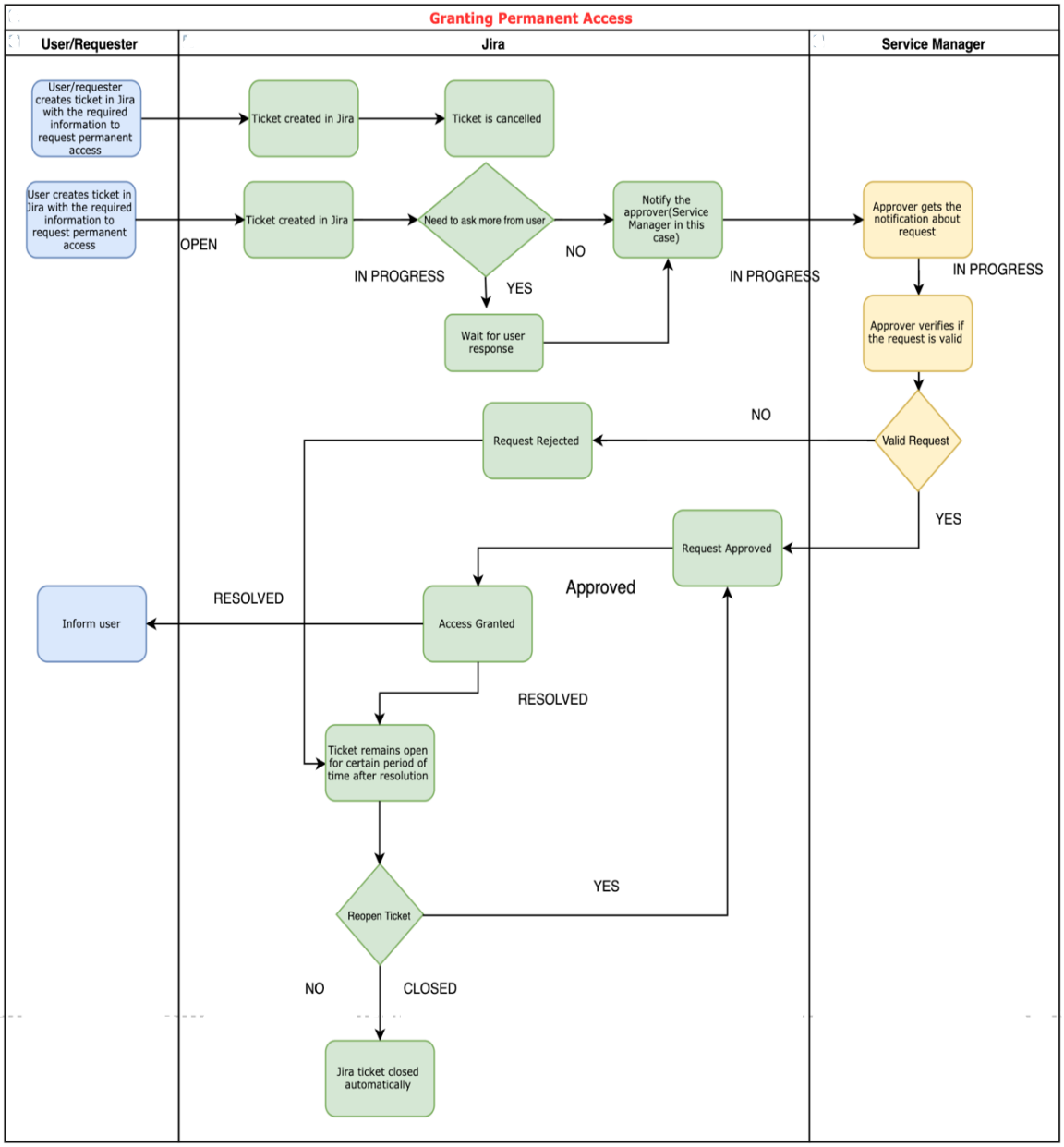

Figure 4.1. Workflow for granting permanent access

Revoking Access

The permanent access is granted for a longer period of time and lasts as long as the user needs it. We have two types of users in this system. First, the customer project team members who need access as long as they are part of the team. If a change in team or responsibility of customer occurs, then revoke of access for that customer is required. Second, users who are not part of the customer project team but requested access to work on a particular task. Once the task for which the access was requested is completed then removal of access rights has to be requested (ISO/IEC-27001, 2013). The removing of access rights can be requested either by the person themselves or by the system owner. There could be multiple cases where system owner might need to request revoking of access such as when he knows that the person is no longer working on the projector as a result of the access review of the system. The removal of access can also be requested through Jira ticket by the following process.

1. The user/requester created a ticket in Jira and provides the following information:
   - Name/Name of person on behalf of whom the request is created
   - Customer name
   - Description (optional)
2. The status of the ticket will be OPEN, and the user will get a notification that an access request has been created successfully.
3. The ticket goes into IN PROGRESS state and if the JSD agent needs further information from the user then comments can be added to ask the user for further information.
4. In the case of revoking of access, no approval is required. Support can revoke the access rights of requester from customer environments.
5. The status of the ticket is changed to RESOLVED and the user is informed about the revoking of rights.
6. The ticket remains in the RESOLVED state for a certain period of time. At this stage, there is a possibility to REOPEN the ticket.
7. The reopening of the ticket might be needed in a situation where the access was revoked but it didn't work. The reopened ticket goes through the revoking of access process again.
8. The ticket is closed automatically after some time in the RESOLVED state.

9. Jira ticket can be canceled at any stage of the process.

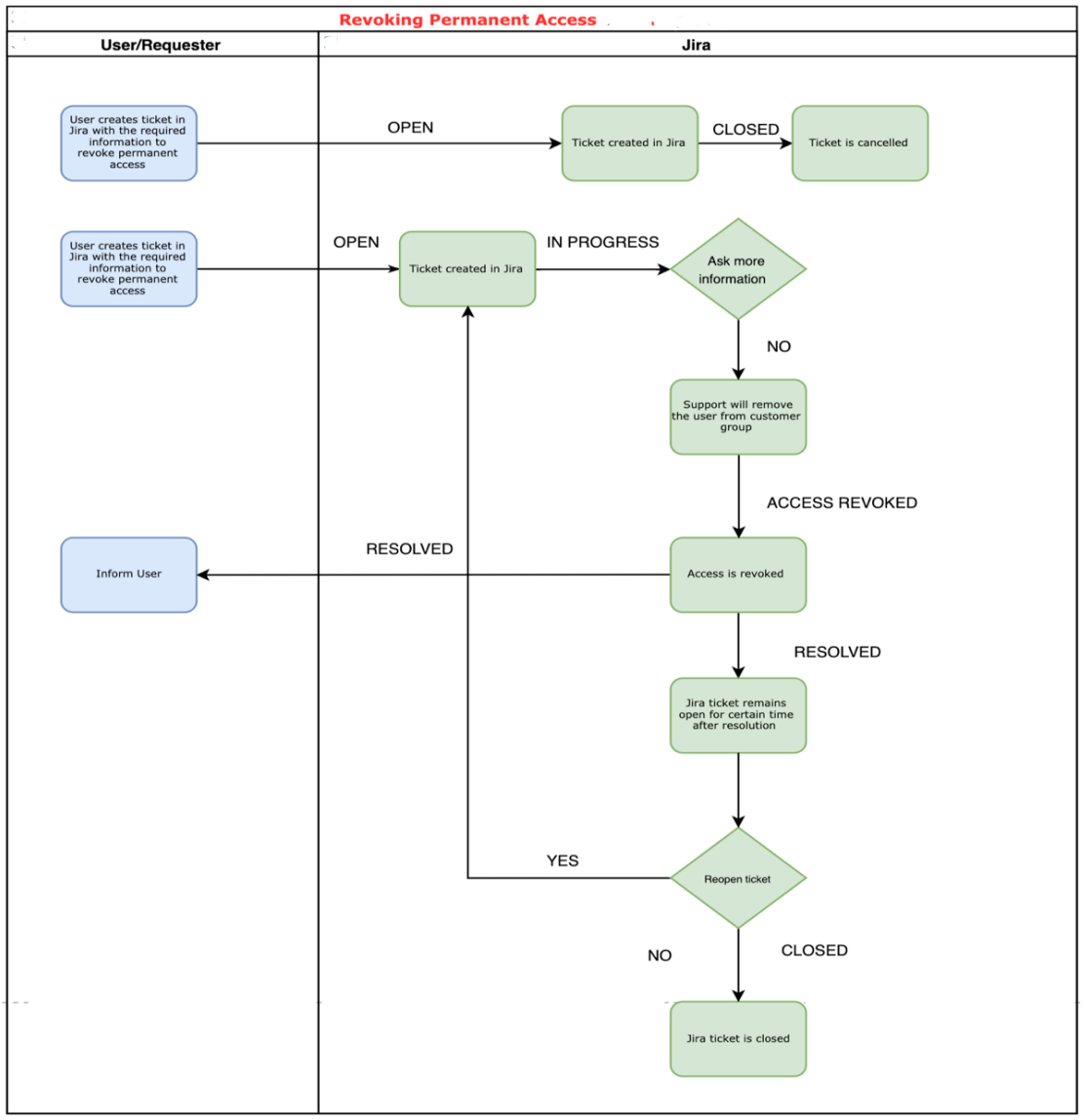

Figure 4.2. Workflow of revoking permanent access

4.6.1.2 Emergency/ Temporary Access

Emergency requests grant access to customer environments for a temporary period of time. These requests are used to get access to work on customer incidents which are most urgent and need people from varying roles to resolve them depending on the type of incident. As discussed in chapter 2, temporal constraint allows having time-based access restriction. Therefore, emergency access is granted for a temporary period of time, there is a temporal constraint of minimum time i.e. 72 hours for which this access is granted. However, the user can request to revoke access any time before 72 hours depending on

the completion of the task. These requests are linked to the customer incidents for which customer create incident issues in customer support system which are the basis of granting access. Therefore, emergency access to customer environments should be revoked while closing the incident issues. This control helps in ensuring that all emergency access is revoked after the issue has been resolved. The emergency access to customer environments for a temporary time can be requested as follows:

1. The requester will create a ticket by providing the following information
    - Name/ Name of the person the behalf of whom you are requesting
    - Reason for access
    - Customer name
    - Description (Optional)
2. The status of the ticket is OPEN and the user will get a notification that access request has been created successfully.
3. As emergency requests are needed quite urgently and mostly linked with the customer incidents, so the process is managed and approved by Support. The ticket goes into INPROGRESS state and then support gets the notification of request being the approver.
4. The approver can assess the urgency of the request if it really requires emergency access or not.
5. If it is not a valid request, then it is rejected and goes to RESOLVED state.
6. In case of valid request, the access is granted and status changes to ACCESS IN PROGRESS.
7. In the case of emergency requests due to their temporary nature, there is a 72 hours timer which keeps the track of the time for which access is in progress.
8. When the timer is about to expire it notifies support. Support can then ask the user if there is a need to extend the access.
9. If the access is to be extended, then the ticket again goes into ACCESS IN PROGRESS state and the timer is reset to 72 hours.
10. If the access is not extended then the access is revoked, status is changed to RESOLVED and the user is informed.

11. The emergency access tickets are linked to the customer incident tickets so that incidents tickets cannot be closed before revoking the emergency access while closing the Jira issues.
12. Jira tickets can be closed at any point of the workflow.

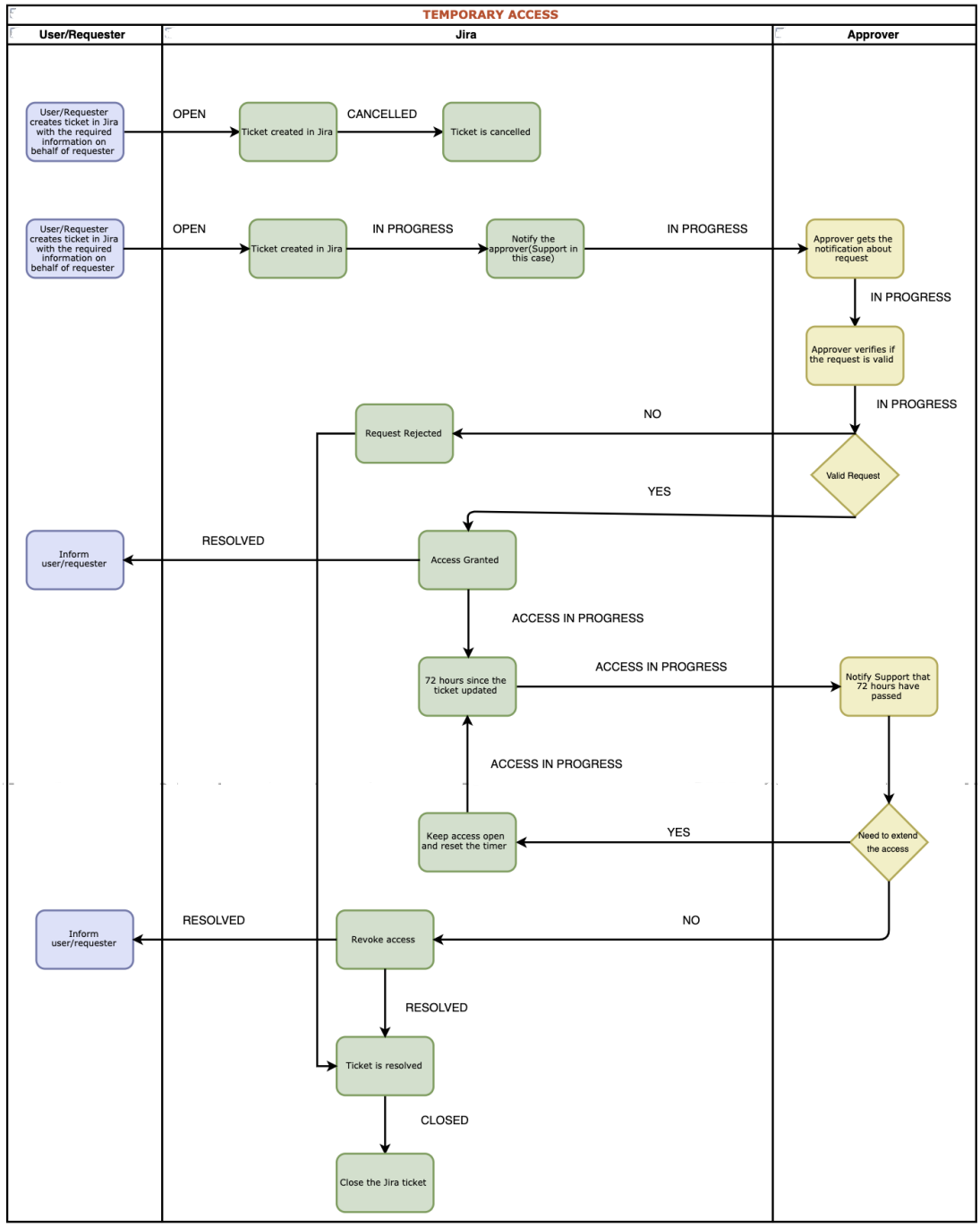

Figure 4.3. Workflow for temporary/emergency access

4.6.2 Internal System Access

The Internal systems are used for different purposes and collectively help the organization to operate. The amount and sensitivity of customer and organizational data also vary in these systems. Since the access rights to internal systems are required depending upon the role definition and responsibilities so access is mainly on the basis of RBAC (Loomis & O'Connor, 2010). Therefore, access to internal systems and applications is managed in multiple ways depending upon the system, role, and responsibilities of employees. Some of the systems are very essential for all employees to work and communicate effectively, some are just needed for certain teams and others can be requested on the need basis. Similarly, varying access levels exist in the systems so based on the need different levels of rights can be requested. So mainly we have categorized the Internal systems into three types based on the access as defined below.

Pre-approved access for all employees

Access to these systems is mostly granted during the on-boarding process. A certain level of access right is granted initially but in case the role demands a different level of access then that can be requested.

Pre-approved access granted to specific teams

Pre-approved means access to these systems is granted without request to the specific team as they need these systems to perform their job tasks. The applications that are pre-approved for a particular team are assigned to the team-based groups in the Identity and Access Management System. Users who are not part of the specific team are not included in the team groups and therefore don't already have access to these systems. Such users can request access to these systems based on their need. Access to these systems is managed by the system owners.

Access needs to be requested from internal IT

The systems for which access is granted by Internal IT support can be requested through Jira. Basic access to some of these systems is pre-approved for employees and assigned at the time of on-boarding. However, as most of the internal systems have different levels of access rights if the user needs wider access e.g. admin rights or some other level of

access, they can create a ticket in Jira and request it thereby providing the reason for access. The access to internal systems can be requested through Jira as follows:

1. The requester will create a ticket by providing the following information
    - Name/ Name of the person the behalf of whom you are requesting
    - Reason for access
    - System/Application name (only request one system in one ticket)
    - Description (Optional)
2. The status of the ticket is OPEN, and the user will get a notification that the access request has been created successfully.
3. The ticket goes into IN PROGRESS state and if the JSD agent needs further information from the user such as the reason for access or level of access rights need, then comments can be added to ask the user for further information.
4. The approver for the internal system is IT support and they are managing the process as well. Approver assesses the validity of the request while the ticket is still in progress.
5. If the request is not valid then the request is rejected, and the status of the ticket is changed to RESOLVED.
6. If the request is valid then the access is granted and the status of the ticket changes to RESOLVED.
7. In the RESOLVED state there is an option to reopen the ticket. In the first scenario, reopening might be required after the request is rejected by mistake or due to some other reason and now there is a need to reopen the ticket. In this case after reopening the ticket goes to the INPROGRESS state where it again goes through the whole process.
8. In the second case, the reopening of the ticket can be required when the access was granted to the system, but it is still not working. In this case, the ticket after reopening will go to the state of request approved and then follows the remaining process.
9. When the ticket is in the RESOLVED state for some time, it will be automatically closed.
10. Internal IT will verify if the request is valid and then approve or deny the request.
11. All Jira tickets can be canceled at any stage of the process.

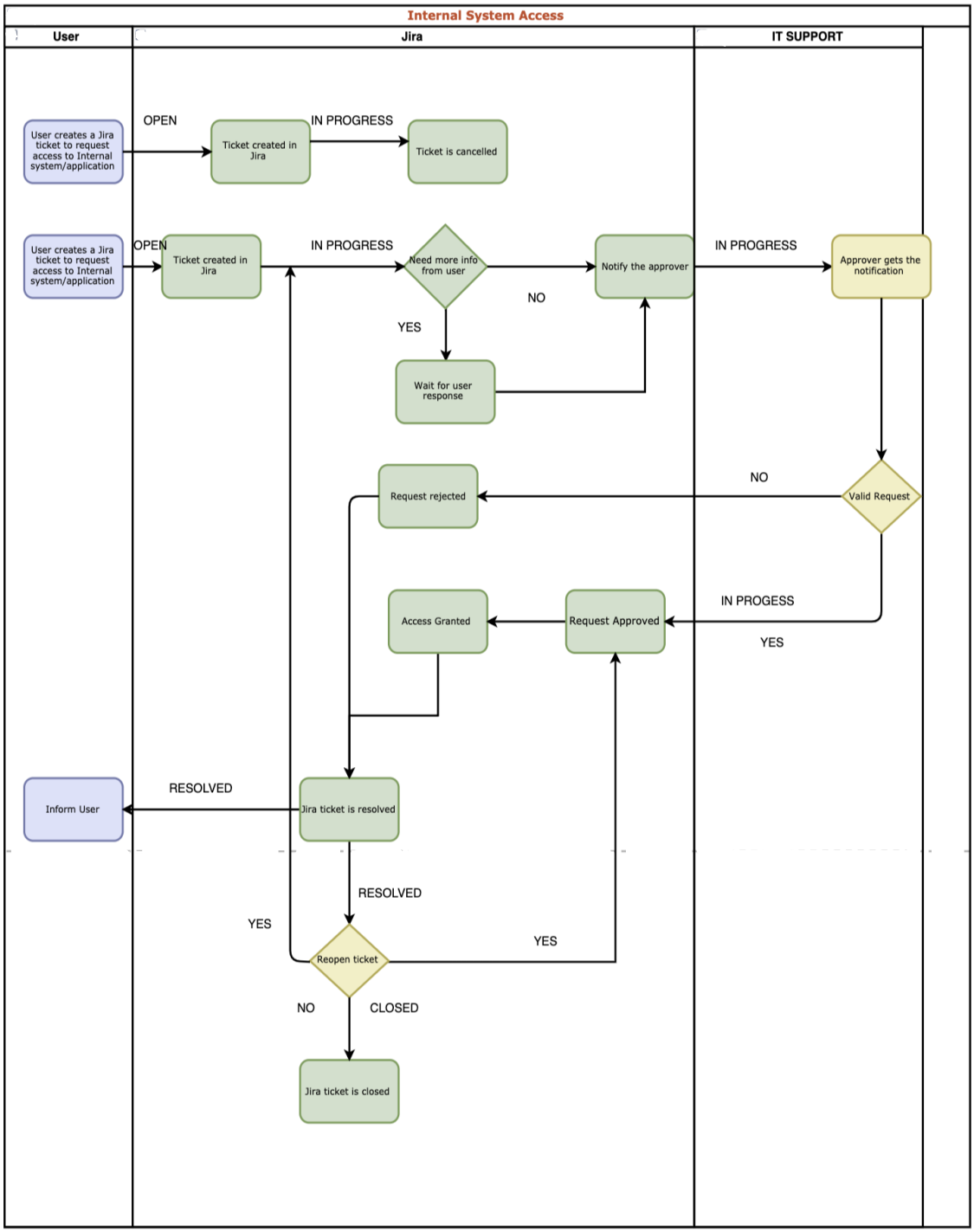

Figure 4.4. Workflow for internal system request

4.6.3 Change of Status

Change of status is another type of service request in Jira. Change of status includes various use cases such as change of role, team, the title that lead to the change of access

rights and other such as change of location, and name. that do not affect user access rights directly (Razieh & Modiri, 2012). The systems that contain user information i.e. HR Management System and Identity and Access Management System are important in the access management process. Therefore, user data/profiles should be kept updated and any changes in user information should be pushed to these systems so that users always have appropriate access rights and if there is some change then access rights are adjusted accordingly. Users or team leads can inform about the changes by creating a ticket in Jira which notifies the relevant teams as a result relevant system are updated. The process in Jira for change of status goes like this:

1. Change of status ticket is created in Jira by user/team lead.
2. Jira agent based upon the type of request and location where the change occurred, assigns the ticket to relevant teams (IITS and People).
3. When the ticket is assigned, relevant teams get the notification.
4. The HR team upon receiving the notification updates the HR Management System.
5. The data is then pushed from the HR Management System to the Identity and Access Management System.
6. Identity and access management system has user profiles which get updated as a result of data push.
7. As the user profile gets updated, the Identity and access management system rules based on user profile add to the new team-based group and remove a user from the old team/department/division.
8. This will change the access rights to the pre-approved team-based systems assigned to the team-based groups.
9. When the relevant Internal IT team gets the notification, they update the Internal systems managed by them.
10. Internal IT also updates the access rights if required due to the change occurred.
11. Notification can be sent to the user informing that access rights were adjusted, and detail can be seen here (Jira ticket URL).
12. In some cases, there is a transition time in which the user still has some responsibilities from the old team. To cater to this scenario, an optional transition field has been added in the Jira ticket.

13. If the user has some transition time, then it should be mentioned along with the team information.
14. For system managed by Internal IT and customer environments, access can be requested by Jira access request tickets.

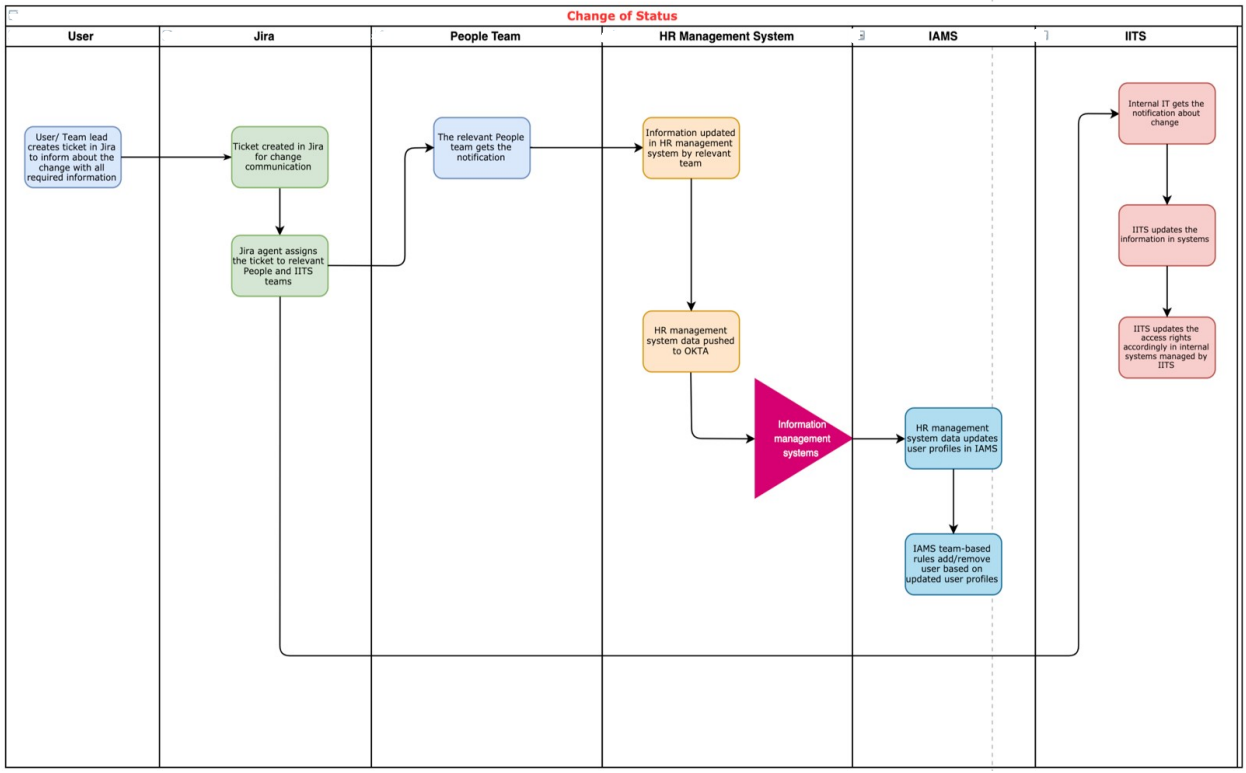

Figure 4.5. Workflow for change of status

4.7 System Interfacing

The access management process can interface to various processes interfacing with IT services. Since we have discussed the system involving in the access process and the process for managing different types of access, it will be good to see how these system interfaces. As the access process is mainly based on user roles so the first system in play is HR Management System that keeps the master data of user attributes like, title/role, team, department, and division. To keep this user data updated, the process of change of status has been designed.

Next, the Identity and Access Management System maintains the user profiles and the data for the user profile is pushed from the HR Management System. These profiles are

further used in rules to maintain various customer and team groups. Jira the ticketing and logging system manages the access lifecycle and tracks the user access. The users in the Identity and Access Management System are pushed to Jira. In this way, the user is able to use the Jira system for requesting and managing access based on their access rights and roles. The integration and data flow between different systems have been depicted in the below diagram.

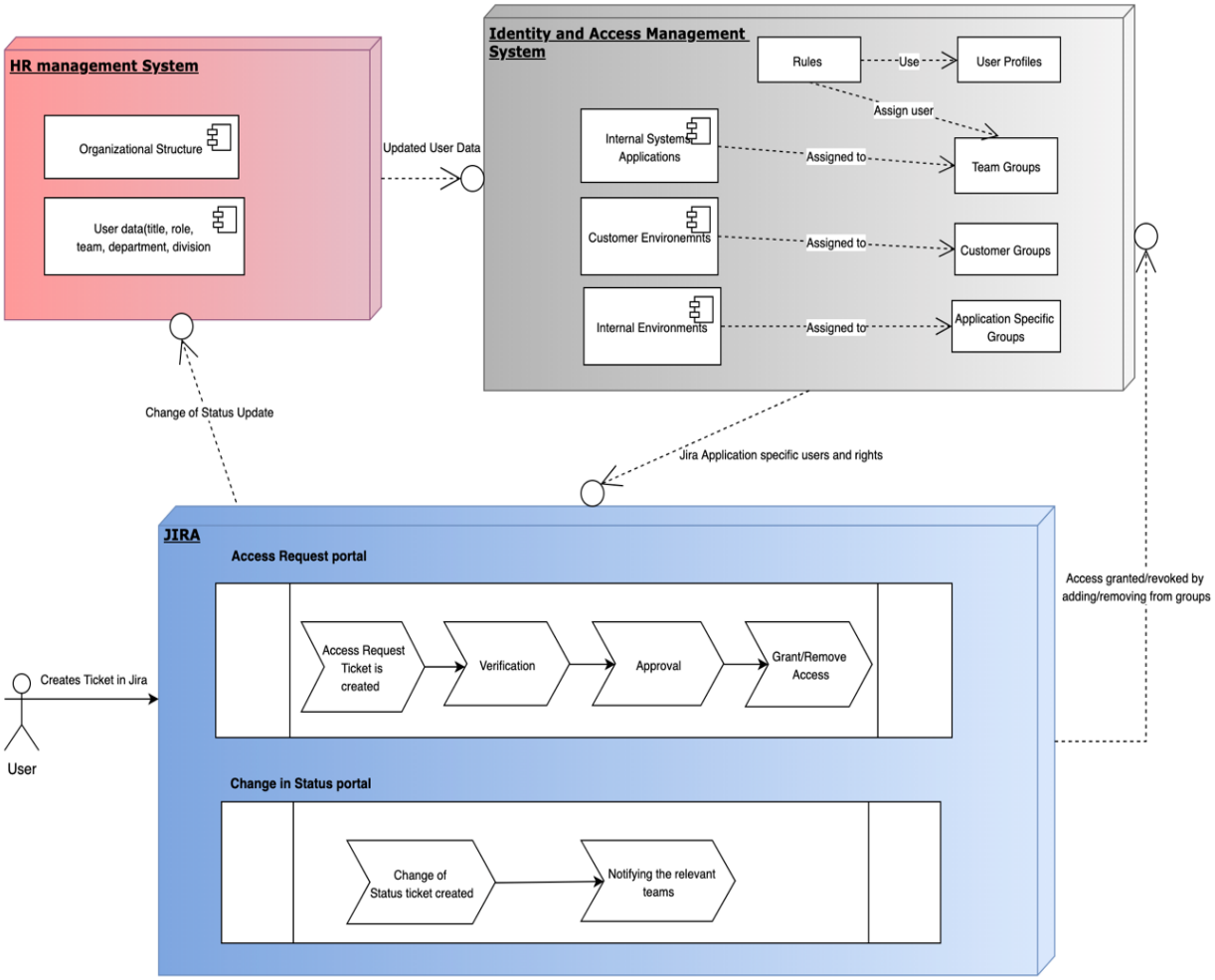

Figure 4.6. System Context Diagram

4.8 Mapping Requirements and Controls

This section discusses the mapping of requirements from security standards with the controls that have been designed to fulfill those requirements. The SOC 2 requirements are integrated with COSO principles. COSO framework is a recognized framework that

is used to evaluate the design and operating effectiveness of internal controls of an entity. There are 17 principles of COSO which are grouped into the categories of communication and information, control environment, monitoring activities, risk assessment and control activities. To compile the requirements regarding access control and to align them in a better way, the COSO principles for SOC 2 have been mapped with ISO 27001 requirements. Below the COSO principles are listed as A, B and C along with the points of focus (represented as A.1, A.2, B.1, etc.) mapped with the relevant ISO clause(s) (represented as A.1.1, A.1.2, B.1.1, etc.) and the organizational controls designed to meet the requirements, have been mentioned (AICPA, 2018).

A COSO-CC6.1

The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

A.1 Point of Focus

Identifies and manages the inventory of information assets—The information assets are identified, inventoried, classified and managed (AICPA, 2018).

A.1.1 Inventory of assets

Information, other assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained (ISO A.8.1.1).

Organizational Control

Assets are maintained in the asset inventory. All customer environments and internal systems inventory are maintained.

A.1.2 Ownership of assets

Asset maintained in the inventory shall be owned (ISO A.8.1.2).

Organizational Control

List of assets along with ownership information is maintained. Information regarding customer environments for each customer is maintained along with the system owner details. Moreover, the inventory for internal systems and applications with their responsible system owners is available.

A.2 Point of Focus

Restricts logical access—logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets (AICPA, 2018).

A.2.1 Management of privileged access rights

The allocation and use of privileged access rights shall be restricted and controlled (ISO A.9.2.3).

Organizational Control

Secure log-on procedures are implemented for all systems and applications required for service delivery. Privilege access rights are granted only on the basis of the need to know principle or if required by the role. These can be requested through Jira portal for Internal system requests.

A.2.2 Information access restriction

Access to information and application system functions shall be restricted in accordance with the access control policy (ISO A.9.4.1).

Organizational Control

The access control process is in place as per the access policy. Access to applications is restricted according to the role-based access model and principles of "need to know" and "least privilege".

A.3 Point of Focus

Identifies and authenticates users—persons, infrastructure and software are identified and authenticated prior to accessing information assets, whether locally or remotely (AICPA, 2018).

A.3.1 Secure log-on procedures

Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure (ISO A.9.4.2).

Organizational Control

Secure log-on procedures are implemented in all systems and applications required for service delivery. the Identity and Access Management System is used to authenticate users before accessing the customer environments and Internal systems. Moreover, the user role that determines the level of access rights is sent while authentication by the Identity and access management system to customer environments.

A.4 Point of Focus

Manages points of access—points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed (AICPA, 2018).

Restricts access to information assets—combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access control rules for information assets (AICPA, 2018).

Manages identification and authentication—identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure and software (AICPA, 2018).

A.4.1 Secure log-on procedures

Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure (ISO A.9.4.2).

Organizational Control

Secure log-on procedures are implemented for all systems and applications required for service delivery. Employee Access Control policy is in place and the Identity and Access Management System is used to authenticate users before accessing the customer and internal systems.

A.4.2 Use of secret authentication information

Users shall be required to follow the organization's practices in the use of secret authentication information (ISO A.9.3.1).

Organizational Control

Employee Information Security Policy requires to use high quality and unique passwords in every system and advice to use password management system.

A.5 Point of Focus

Manages credentials for infrastructure and software—new internal and external infrastructure and software is registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required, or the infrastructure and software are no longer in use (AICPA, 2018).

A.5.1 User access provisioning

A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services (ISO A.9.2.2).

Organizational Control

Access to systems holding confidential data is granted as per role and on the need to know basis by access requests. No more access, than what is needed to fulfill the assigned tasks is granted. Access is not granted before approval and requests are approved by system

owner or person with delegated system owner duties. Emergency access to investigate escalated issue can be granted by the 24/7 Support team when the urgency of the issue justifies the access. Emergency access request must be linked to issue.

A.5.2 Removal or adjustment of access rights

The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change (ISO A.9.2.6).

Organizational Control

Emergency access requests must be closed, and the access revoked while closing the issue. System owners are yearly reviewing access rights for systems holding confidential data as per the User Access Management Process. Moreover, privileged users are reviewed at least every 6 months as per the Access Control Policy. The change of status process is also in place that leads to the adjustment of access rights according to the change.

B COSO-CC6.2

Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

B.1 Point of Focus

Controls Access Credentials to Protected Assets—Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian (AICPA, 2018).

B.1.1 User registration and de-registration

Formal user registration and de-registration process shall be implemented to enable assignment of access rights (ISO A.9.2.1).

Organizational Control

Access to systems holding confidential data is granted on a need basis by access requests. No more access, than what is needed to fulfill the assigned tasks is granted. The access requests are approved by the system owner. Removal of the access process is in place once the access is no longer needed. Moreover, access provided by emergency access request is revoked while closing the issue.

B.1.2 User access provisioning

A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services (ISO A.9.2.2).

Organizational Control

Access is not granted before approval. Access requests are approved by the system owner or person with delegated system owner duties. Emergency access to investigate escalated issue can be granted by the 24/7 Support team when the urgency of the issue justifies the access. These access request must be linked to issue.

B.2 Point of Focus

Removes access to protected assets when appropriate—processes are in place to remove credential access when an individual no longer requires such access (AICPA, 2018).

B.2.1 Removal or adjustment of access rights

The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change (ISO A.9.2.6).

Organizational Control

Emergency access requests must be closed, and the access revoked while closing the issue. Access rights are adjusted or removed upon change of status or termination of the employment. There is a specific offboarding process for handling the termination.

B.3 Point of Focus

Reviews Appropriateness of Access Credentials—The appropriateness of access credentials is reviewed on a periodic basis for unnecessary and inappropriate individuals with credentials (AICPA, 2018).

B.3.1 Review of user access rights

Asset owners shall review users' access rights at regular intervals (ISO A.9.2.5).

Organizational Control

System owners are yearly reviewing access rights for systems holding confidential data as per the User Access Management Process. Jira also logs and track access activities that are reviewed.

C COSO CC6.3

The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

C.1 Point of Focus

Creates or modifies access to protected information assets—processes are in place to create or modify access to protected information assets based on an authorization from the asset's owner (AICPA, 2018).

C.1.1 User access provisioning

A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services (ISO A.9.2.2).

Organizational Control

Access to systems holding confidential data is granted on a need basis by access requests. No more access, than what is needed to fulfill the assigned tasks is granted. Access requests are approved by the system owner or person with delegated system owner duties. Approval must be based on business reasons justifying the need to access. Emergency

access to investigate escalated issue can be granted by the 24/7 Support team when the urgency of the issue justifies the access. Access request must be linked to issue.

C.1.2 Removal or adjustment of access rights

The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change. Emergency access requests must be closed, and the access revoked while closing the issue. Access rights are adjusted or removed upon change or termination of the employment. There is a specific offboarding process for handling termination (ISO A.9.2.6).

C.2 Point of Focus

Removes access to protected information assets—processes are in place to remove access to protected information assets when an individual no longer requires access (AICPA, 2018).

C.2.1 Review of user access rights

Asset owners shall review users' access rights at regular intervals. Emergency access requests must be closed, and the access revoked before closing the issue (ISO A.9.2.5).

C.2.2 Removal or adjustment of access rights

The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change (ISO A.9.2.6).

Organizational Control Access rights are adjusted or removed upon change of status or termination of the employment. There is a specific offboarding process for handling the termination.

C.3 Point of Focus Uses Role-Based Access Controls—Role-based access control is utilized to support the segregation of incompatible functions (AICPA, 2018).

C.3.1 Segregation of duties Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets (ISO A.6.1.2).

C.3.2 Management of privileged access rights The allocation and use of privileged access rights shall be restricted and controlled (ISO A.9.2.3).

Organizational Control Access control is based on role-based access control model. Access rights to customer environments and internal systems are granted based on roles. Segregation of duties has been implemented through RBAC. Moreover, privileged rights have to be requested and privilege users are reviewed at least every 6 months as per Access Control Policy.

Chapter 5

5 Implementation and Testing

The purpose of the access control process is to manage access to services based on information security policies. Moreover, making the access management process efficient so that requests for granting, changing or restricting access rights are properly managed. Access management process also enables monitoring the access to services and to ensure that the access rights are not being misused. The systems in the scope of this process are customer environments that contain critical customer sales and inventory data and organizational internal applications.

All the system discussed in chapter 3 were involved in the implementation of the access management process. Some processes, procedures, and roles already existed in the organization. Customer project teams and other users working on customer projects already have access to customer environments. Before the implementation and starting to use the new access process in place, it is required to define the roles based on their access needs and to include existing users in the system. As the process is implemented based on role-based access control (RBAC) model (Sandhu et al., 1996), creation of roles and assigning those to appropriate people is the first step towards including existing users in the system based on their roles in the organization.

5.1 Creation of Roles

The access policy is designed around role which is a semantic construct. Roles have associated permissions and users are members of roles, therefore, acquiring those permissions (O'Connor & Loomis, 2010). There are specific roles that are authorized to have access to particular customer environments. Therefore, the process goes in a way that first, we define the roles based on the organizational structure and requirements.

The organization has a hierarchical structure that consists of four levels starting from top to bottom.

1. Division/Function
2. Department
3. Team
4. Sub-team

There are multiple types of groups based on the hierarchical structure, roles, and requirements of work. As different roles from different teams work together on a customer project so there are specific groups for customers as well.

1. Division groups
2. Department groups
3. Team-based groups
4. Sub-team-based groups
5. Customer project team-based groups

As not all of them but specific roles from the above-mentioned groups need specific access to customer environments and data. Therefore, these roles who need to be authorized to access customer environments were combined in different groups to assign permissions based on their requirements.

- Technical Support
- Business Support
- Solution Consultant
- Business Analyst
- Customer Project team member
- Service customer team member
- Industrial customer team member
- Solution services team member
- Employee
- Contractor

The support role i.e. technical and business support based on their responsibilities of solving customer incidents and providing support which can occur at any time need access to all customer environments at all times. The users assigned to these roles also

get the permissions when they are in that particular support role. Similarly, the solution consulting and business analyst roles require wider access like support role as per the requirements of their work and to fulfill their responsibilities. The solution services role requires access to all except some big customers, so their needs also differ from other roles.

The customer project team member role forms the project team and needs access all the time to work on customer-related tasks. However, the users in this role have varying titles such as service manager, project manager, technical consultant, and account manager but the main role here is customer project team member role which authorizes them to have access rights to that particular customer. In addition, the role for users who need access to customers that are categorized as service phase and industrial customers are named as service customer team member and industrial customer team member role. If users are assigned to these roles, they have permissions to access all service or industrial customers respectively.

The employee role is a generic role which is assigned to all users who are organizational employees so that they can be given access to particular training and internal environments which does not contain actual customer data but some simulation of customer environments and best practices. Moreover, the organization also has some contractors who need access to particular services based on their contracts, so this role has been constructed for them.

5.1.1 Groups, Role, and Permissions

IAMS is the access management system where all groups, roles, their associated permissions and applications assigned to them are being managed. The roles mentioned in the last section were created based on their particular requirements to have access to customer and internal applications. Now based on the requirements of these different roles, groups were created in IAMS that contained these roles or combination of roles. This approach makes it easier to assign varying permissions to groups and then based on the need's user are associated with those roles. In this way, upon changing the role, the relevant access rights are also adjusted for the user accordingly. The following groups were created in IAMS with relevant roles and permissions assigned to them.

Organization-support

Roles: The technical and business support roles are assigned to this group.

Permissions: Access to all customer environments at all times.

Organization-support-Internal

Roles: All users and roles are assigned to this group.

Permissions: Users can access all internal environments, simulation and training environments. Moreover, environments with best practices to be implemented in customer environments but do not contain any customer data are also accessible by this group.

Organization-support-customer

Roles: only customer project team member role is assigned to this group

Permissions: All customer environments and data for that particular customer are accessible by this group.

Organization-support-service-customer

Roles: Only service customer team member role is assigned to this group.

Permissions: All customers in the category of service customers are accessible by this group.

Organization-support-solution-service

Roles: The role of solution services team member is assigned to this group.

Permissions: All customers except some are accessible by this group.

Organization-support-Industrial-customer

Roles: only industrial customer team member role is assigned to this group.

Permissions: This group can access only specific industrial customers.

Organization-support-country

Roles: The team member role for a particular country team is assigned to this group for instance team member of team France is assigned to group organization-support-France.

Permissions: The roles in this group can access all customers that belong to a particular country.

Organization-employees

Roles: All employees have the employee role assigned to them, so this group contains the employee role.

Permissions: The group can access particular applications that are required to be accessible by all employees.

Organization-contractors

Roles: All contractors have the contractor role assigned to them, so this group contains the contractor role.

Permissions: The group can access only those applications that contractors need to access.

Team-based groups

Roles: The team-based groups contain team member roles.

Permissions: The team-based group has the access rights to use particular applications that are required for a particular team to fulfill their job tasks.

Application-specific Groups

Roles: Application specific groups contain different roles based on their need to access the application.

Permissions: A particular application group can access that application. However, different roles can have varying access rights.

5.2 Including Existing Users in System

Some processes and procedures to access customer environments and data already existed in the organization. For such an organization that has processes and procedures already in place and being used, the inclusion of existing users in the newly designed process is a necessary step before actually switching to that process (Razieh & Modiri, 2012). When the new access process will be in place it will be used for new access requests. Nonetheless, to ensure that appropriate users are assigned to these roles a review process was conducted. The main focus here is the customer project team or users who are not part of the team but currently working on that particular project.

5.2.1 Aggregating Data

The data needed for the implementation of access management process was gathered from multiple sources and then aggregated to get the final needed information. The data was gathered from various systems including those discussed in chapter 3 and some mapping was done to get the final list. The following process has been followed.

1. Initially, a list of all users who have accessed the customer environments in last few months was gathered along with the customer name, applications name, technical consultant name, last login date, time and system owner details. The system owner for customer environments is service manager who has also the role of approver of access to a customer.
2. In the next step, some filtering was done in which internal environments were removed as they do not belong to the category of customer environments. Moreover, roles with special cases such as Technical and Business support roles were removed as we already identified that they need access to all customer environments to perform their function smoothly.
3. The data was then aggregated to a customer-user level which means that all users who have accessed a particular customer were listed against that customer.
4. The system owner (Service Manager) was included in the service manager column for each customer.
6. As each particular customer will have its own Customer project team-based group so these groups were also added next to each customer.

5.2.2 Reviewing

The review of the data was done in two phases. In the first phase, the system owners were provided access to the list for review where they were needed to review each user in the list if they need access to a particular customer. The criteria for review was that only the users who are part of the customer project team i.e. are assigned to the role of the project team or users currently working on some customer related task, should have access to the customer environments. Those who need access were marked as "needed" whereas, for those who should not have access, status was changed to "not needed". Moreover, the system owners also added missing members of the project team or missing customers on the list. In the second phase, the project team members did the review to ensure they are included for all customers to which they need access. If the project team members find themselves missing from the list for some customer, they can ask the system owner to include them (Xu, 2017).

5.2.3 User ID Mapping

The Identity and Access Management System that maintains all the users and applications to which they have access. Access to customer environments and all applications is managed in this system. The identifier in the Identity and Access Management System that uniquely identifies each user is known as the user ID. As the reviewed list of users with the customer environments to which they are authorized to have access was available, so user ID was required to map the users in an access list to implement the access restrictions in the Identity and Access Management System. The users and their IDs were extracted through scripting.

The list of users and IDs from the Identity and Access Management System was mapped with the list containing users and customer to which they should have access based on their role. The resulting list has all the customers, users who are authorized to have access to these customers based on their roles, users that should be removed from having access, system owner (Service Manager) of the customer environment and user IDs of all users.

5.2.4 User Profile Mapping

The HR Management System maintains the master data for all user related attributes such as title/role, team, department, division, and manager. This information provides the basis for RBAC as implementing RBAC requires appropriate and up-to-date information regarding user profile attributes. The user data consisting of all user profile attributes from the HR Management System was mapped with the user ID to push this information to the Identity and Access Management System for each user. Initially, there was one-way integration between the Identity and Access Management System and the HR Management System such that only the identity and access management system was able to push data to the HR Management System. Due to the lack of this two-way data push, for the first time, the mapping of user profile data was done through excel. Later, to keep the user profile in the Identity and Access Management System up to date, a script was scheduled to keep pushing the updated user profiles from the HR system to the Identity and Access Management System. However, to have a permanent process in place, the integration is in progress where the data between HR Management System and the Identity and Access Management System can be pushed both ways.

5.3 Users Assignment

The Identity and access management system is used for the centralized management of authorization of resource in the target systems that are distributed across the organization. It basically creates and manages the mappings between the system level user accounts, groups and their membership with enterprise-level users, roles and their memberships. This is executed by the creation and deletion of user accounts and groups. Moreover, it also assigns user accounts to the groups. The fundamental parts of the mapping of system access permissions to RBAC semantics at the enterprise level are the user's IDs and groups. The mapping of an enterprise view onto a system level group is done by assigning users to groups that are assigned to and inherited by its corresponding role. In such a technique instead of assigning permissions to roles, they are assigned to groups which are then mapped with roles organized into a role hierarchy.

5.3.1 Assigning Users to Team-based Groups

Each team in the organizational hierarchy has a team group. The users with role team member are assigned to the team-based groups based on teams to which they belong. Moreover, all applications or tools which are pre-approved for a particular team means that they need these applications and tools to perform their job tasks, are assigned to the team-based groups. Each user has a profile in the Identity and Access Management System which contains the user team, department, division, and title. These groups are managed through rules which are based on the user team information. Users are automatically added and removed from team-based groups based on the rules. The team-based groups are also the source to manage access to internal applications or tools.

5.3.2 Assigning Users to Other Groups

The access list contained all users who should have access to a particular customer, the user IDs and the customer group in which they have to be added (Hu et al., 2006). Script used a CSV file and reads a list of users and their customer groups. To find the relevant customer application that also has to be assigned to the customer group, a search criterion was included in the list. The script reads the search criteria and based on that looks for all applications containing the search criteria in their name. It created the customer group on the run, then assign each user to their particular customer group and then assigns the

groups to applications. The script also saves all applications that were found based on search criteria along with their group ID in the script directory. So, after running the script, all customer groups in the Identity and Access Management System were created. All users with role customer project team member and all applications related to that customer are assigned to the particular customer group.

Similarly, all groups i.e. Organization-* which have been discussed in the above section were created through a script. Users are assigned to the relevant group based on their roles and applications which they are authorized to access.

5.3.3 Setting Rules

Rules in Identity and Access Management System are also set for these groups to handle different cases (Hu et al., 2006). For instance, all existing employees should be added to the group organization-support-internal and every new user should also be automatically added to this group. To manage this requirement the rule is created so that if a user contains for instance "abc.com" then assign to the group Organization-support-internal. In this way, all user is added to this group as they contain abc.com in their email addresses. Furthermore, if the certain case requires whole divisions/departments/team to be assigned to a group then the rule can be created for instance if user.team contains " Support" then add to organization-support.

5.4 Implementation In Jira

The creation of groups and rules in the Identity and Access Management System and addition of existing users as per their roles in relevant groups was followed by implementation of workflows in Jira. Jira is a platform on which applications and products can be built to plan, manage and track project. It allows for creating different projects based on organizational requirements (Atlassian, 2019). As discussed in chapter 3 that Jira has three products i.e. Jira Core, Jira Software and Jira Service Desk. Jira Service Desk was most suitable to meet the needs of this project. Jira Service Desk is a helpdesk request tracker. It allows to receive, manage, resolve and track requests. Users can submit their request in a portal and Service Desk organizes and prioritizes these requests. Teams can keep a track to resolve requests as per their goals and priorities. Similarly, filters and alarms can be set to ensure that urgent requests are being resolved first.

One Jira Service Desk can have one or multiple types of service requests. Access requests and change of status requests were two main types of service requests that were implemented in a single Jira Service Desk to ease the management of all access-related task in one project. This approach minimizes confusion and provides users with a single portal where they can create all access-related requests. Moreover, it allows access requests and change of status requests which ultimately leads to change in access rights for some cases, to manage and track in one project. The logging and tracking of these requests are one of the most important parts of the whole process and a major requirement from security standards as well.

Although the main types of service requests were access requests and change of status requests, the access requests can be further categorized as the access requests of customer environments and access requests for internal systems. So basically, in total three types of service requests were implemented in one Jira Service desk.

5.4.1 Jira Workflow Implementation

The way tasks and processes are managed in Jira is through workflows. A workflow maps out the steps and statuses that a task can go through and defines the process. Only Jira administrator can create and edit the workflows. The higher-level process to implement a workflow in Jira is the same so the same process was followed for the implementation of all workflows designed in chapter 4.

5.4.1.1 Workflow components

A Jira workflow has the following components (Atlassian, 2019).

Status: It represents the current state and aligns usually with the process stage such as notifying, approving or review.

Transition: These are the action due to which task move between statuses such as sent for Approval.

Resolution: When the task is finalized, resolution closes the issue and shows the final state of the issues such as Access Granted.

5.4.1.2 Workflow Creation

Once the mockup or designed workflow is available, the creation of workflow in Jira is not so difficult. The workflow creation process in Jira goes as follows.

1. To create a Jira workflow, go to Project>Project Settings> Workflows>Add Workflow.
2. It gives the option to Add existing workflow or from Atlassian Marketplace. Click Add Existing Workflow**.**
3. Each request type in a service desk is based on an issue type. A single 'type' of issue can be the basis for many different request types. For example, the Access-Request issue type serves as the basis for both the Customer environment access request and Internal system requests. Select the Issue type for the workflow.
4. A new workflow is created with the issue type Access Request and Jira Service Desk default template.
5. Now it can be edited to add status and transitions.
6. Click on the status and then you can edit the name of the status, description, and category (position in the lifecycle).
7. Similarly, click a transition and a window will pop up where you can edit it.

Adding Fields

Fields track attributes that surround each issue type. These enable teams to track data and make the search and filtering process easier. Jira Service Desk has a lot of built-in fields that can be used in the workflows. in addition to the built-in fields, Jira application lets you create custom fields. These fields are optional so no need to change existing issues as they contain no value for the newly defined custom field even if it is defined as default.

To add the existing fields the following process was followed.

1. Go to the Jira project for which you want to edit the fields e.g. Access Request Service Desk
2. Now on the left side go to Settings.
3. On the next page, you will see all the request types. Here you can see the option to Edit fields.
4. On the upper right corner, you will see the Add a field option.

5. All the available fields for the issue type will be shown. You can select the field and then click Apply.
6. The field will be added in the visible field list and now you can set the field Display name, it is required(yes) or optional (No), any text for field help and set them to be visible or hidden.

To add custom fields, the following process is followed.

1. To configure a filed, Select the Jira icon () > Jira settings
2. Now select >Issues.
3. Under the Issues>Fields>CustomFields, you can see all custom fields. On the upper right side, Add Custom field can be used to add a new custom field.
4. If you click on Add custom field, the following window will appear where you can select the type of field.
5. Click Next. Now write the name and description of the field. Click Create.
6. Now associate the field to the appropriate screens before it will be displayed. Select the screen from the list and then scroll down to the end of the page and click Update.
7. Now you can search in the search tab and see the custom field just created with the settings.
8. Now if you go to the project for which you have created the custom field e.g. Access request service desk project and then select Project settings>Request types>Edit fields
9. On the next page, select Add a Field and now select the field on the window that appears. Click Apply**.**
10. It will appear in the list of fields and you can do the settings now.

5.4.1.3 Workflows in Jira

The workflows implemented in Jira based on the designs in previous chapter can be seen in the below figures. These workflows depict the whole process and different phases through which an access request pass.

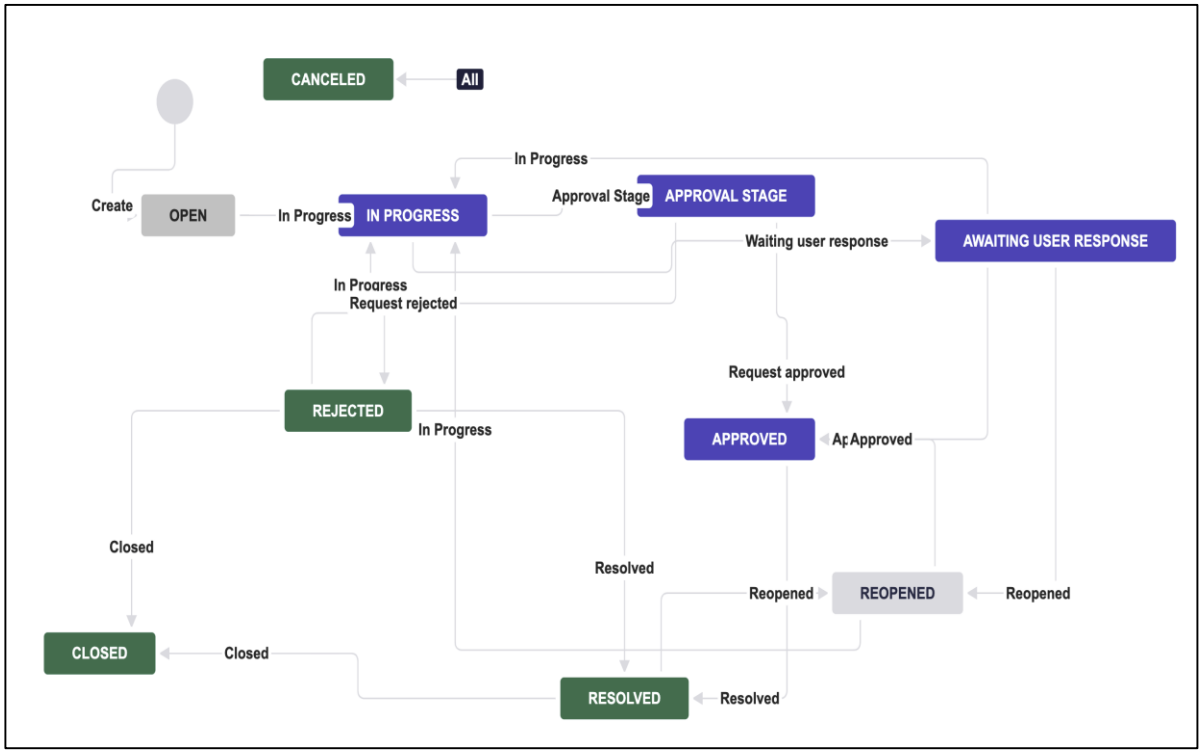

Figure 5.1. Permanent access request workflow in Jira

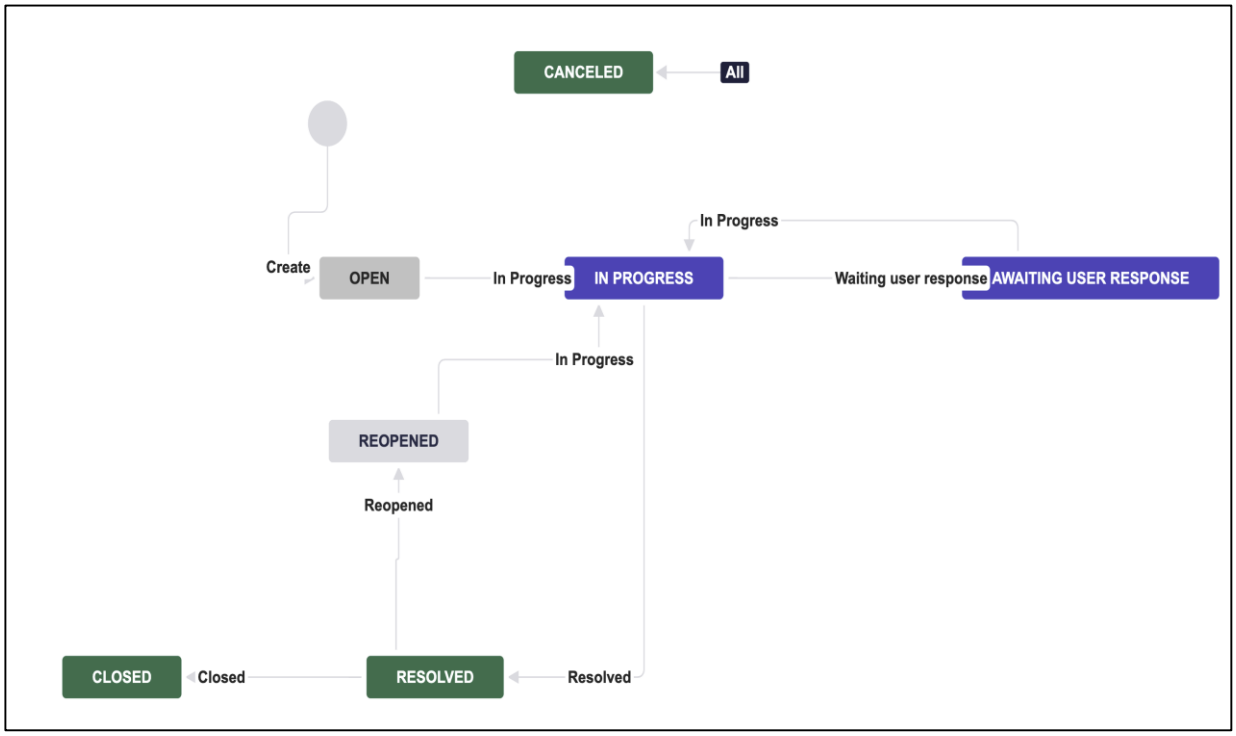

Figure 5.2. Permanent access revoke request workflow in Jira

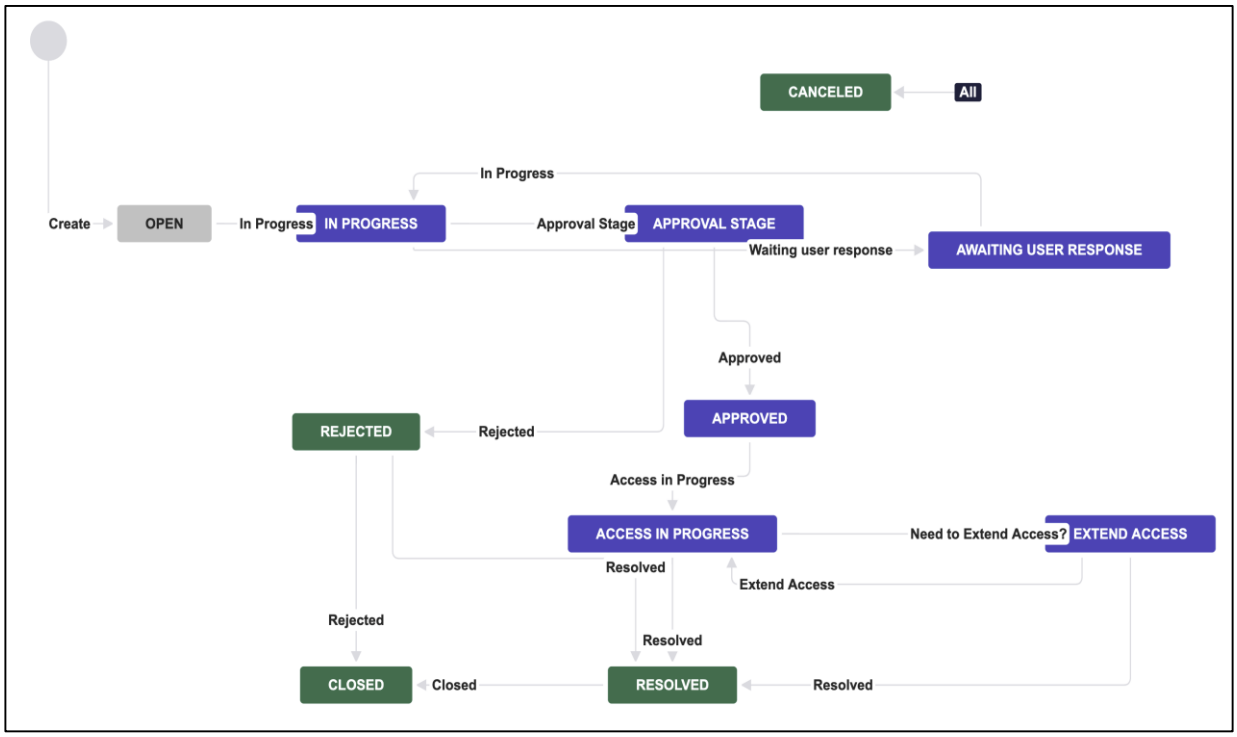

Figure 5.3. Emergency access request workflow in Jira

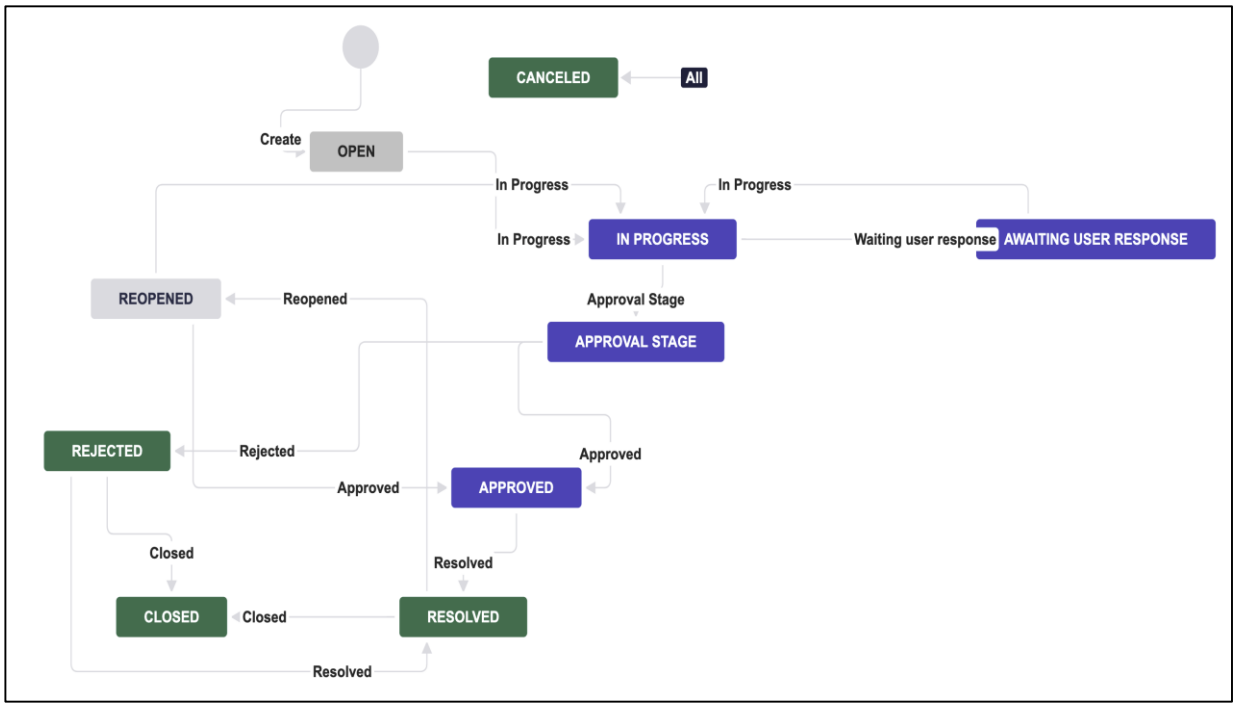

Figure 5.4. Internal systems access request workflow in Jira

5.4.2 Jira Request Portal

Using the above method, the workflows for all Jira Service Desk request types were created. To enable the users to create a request a Jira request portal was created which links to the above workflows. The access to Jira portal is also managed through the Identity and Access Management System. When a user needs to create a request, he/she can go to the request portal and login with their work email address through Identity access management system. Once the user is logged in, all available types of requests for which the user can create ticket are displayed i.e. Permanent access, Removal of access, Emergency access, and Internal system access requests.

User can click on the selected request type as a result of which the request page loads and the next page asks for the needed information for request generation. For instance, if a user clicks on the Request Permanent Access to Customer Environments then the following page appears. User needs to add his name or if creating the ticket on the behalf of requester then adds the requester name. Similarly, customer name for whom the access is required, the reason for access and some description is added. As currently, no database is available which contains the master data for all customers, so an up to date list of users is maintained by the service desk agents. However, in future, the customer database will be linked in a way that it fetches the standard and updated customer names to be displayed in the selection list.

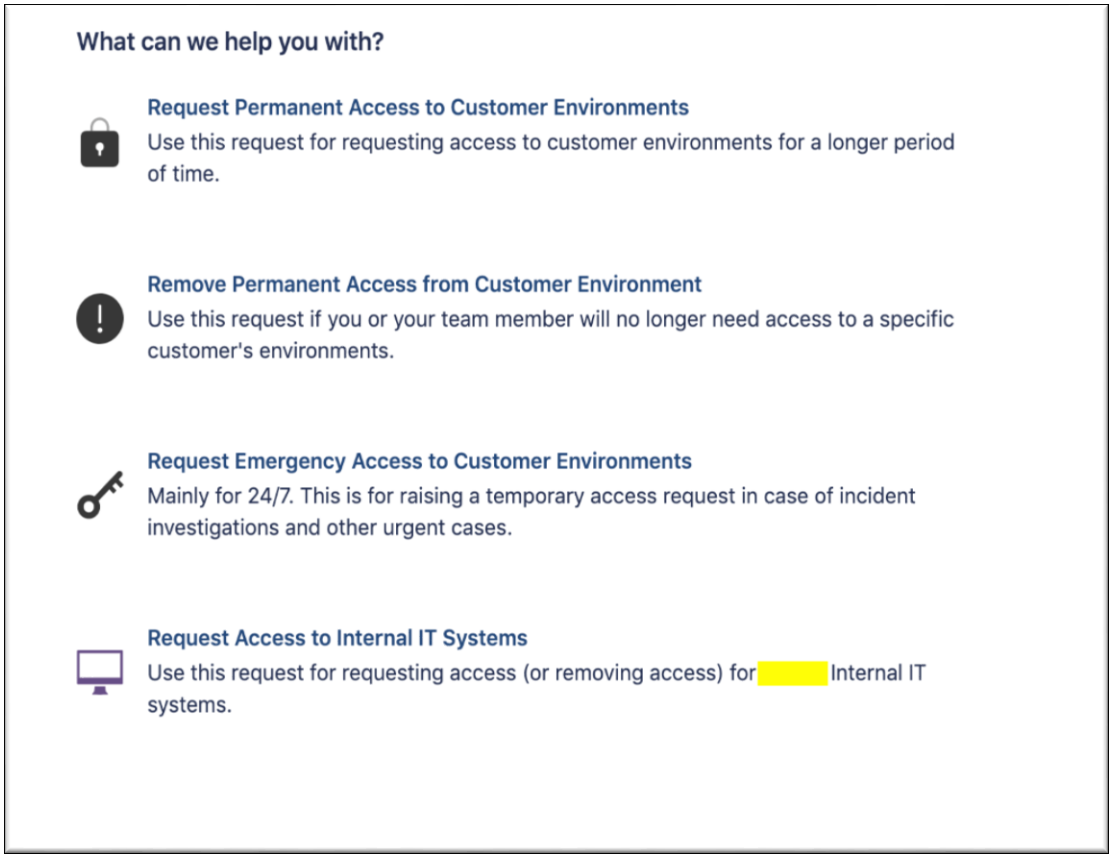

Figure 5.5. Jira request portal

Once the user fills all the details and clicks send, the ticket is created in the Jira request portal. The user receives an email that the Service Desk got the request and it will be processed soon. The user gets the notification both through email and on Jira portal where they can check notifications. The ticket is processed by the Service Desk agent. The ticket goes through different statuses throughout the ticket lifecycle. User is notified upon granting/revoking of access rights and rejecting/reopening of access requests.

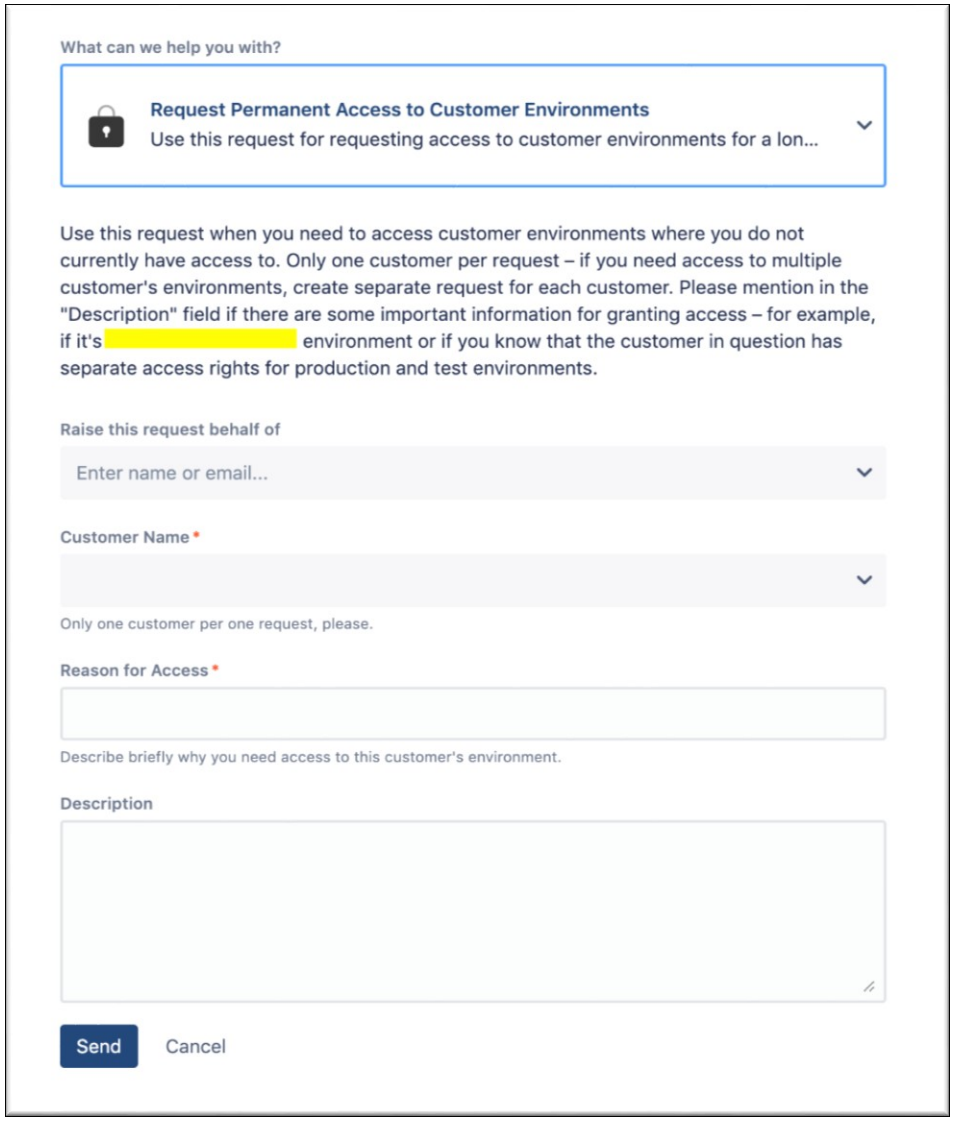

Figure 5.6. Fields in Jira request ticket

5.4.3 Logging and Tracking

As there are multiple types of service requests in one Jira Service Desk, queues can be created to ensure that teams are working on processing the right type of requests. In this way, it helps to organize the requests to be displayed to a particular team. Apart from the ease of management it also enables privacy in the project so that the requests which are destined for one particular team are not visible to other teams. This is achieved by restricting the queue access to a selected group of users. For instance, the request for internal systems should be only visible to Internal IT Support team whereas the requests to customer environments should be displayed for Support team only.

Although the Service Desk project has default queues, customized queues can be created with the required fields as columns and request type. In our situation, three different queues were required i.e. Internal system request queue, Customer environment access request queue and Change of status request queue. The main reason is that all these requests are managed by different teams which act as service agent for the project. As there is no need for one team to view the request of other teams, filtering is required to enable privacy. The internal system requests contain information about the access rights of users in various internal applications across the organization. Similarly, the access request to customer environments have details about users and their access to customer's critical data.

Moreover, the change of status request contains a lot of user personal information which is confidential and only relevant people should be notified. In addition, queues and filters are also quite useful as audit logs. As logging and tracking is an important part of the access control process to efficiently manage access, identify abnormalities and for forensic investigations. Moreover, for auditing purpose, these kinds of logs are quite valuable. Therefore, the queues were created to log issue type, creation date, updated date, access requester, access approver, who granted access, system/customer name, and duration.

5.5 Testing

Access control is a sensitive area for an organization whose operations are mostly dependent on access to customer environments and data. Moreover, a lot of other processes are also directly or indirectly connected to access to environments and applications. Therefore, it was not simple to apply access restriction for the whole organization abruptly. To make the access restriction process smoother, first testing was done in multiple phases and after fixing the issues highlighted during the test process the project went into production.

5.5.1 Phase 1

In the first phase, the focus of testing was the access request process through Jira ticketing system. This was done to ensure that the process is working as expected and to find out

if there are some issues to be fixed before going live with the project. All types of access requests were tested by possible test cases.

Internal System Requests

Test case

- End user-1 to create a ticket: New access
- Internal IT agent to process the ticket (and to approve it).
- End user to see which notifications he receives in the process.

Test case

- End user-2 to create a ticket: New access
- Internal IT agent to process the ticket (and to decline it)
- End user-2 to see which notifications he/she receives in the process

Test case

- End user-3 creates a ticket: Remove accesses
- Internal IT agent to process the ticket (and to approve it)
- End user-3 to see which notifications he receives in the process

Permanent Access Requests

Test case

- End-user-1/requester to create a ticket for herself: New access to customer environment
- Support agent to look up the approver (Service Manager of the customer)
- Approver to approve it in the portal
- 24/7 support agent to add requester in the correct customer group in the Identity and Access Management System
- Support to resolve the ticket
- End user-1/ requester to see which notifications she receives in the process

Test case

- End-user-2/requester to create a ticket for herself: New access to customer environment
- Support agent to look up the approver (Service Manager of the customer)
- Approver to decline it in the portal

- Support to resolve the ticket
- End-user-2/requester to see which notifications she receives in the process

Test case

- End-user-3/requester to create a ticket for herself: Remove from the customer environment
- Support agent to process the ticket
- End-user-3/requester to see which notifications she receives in the process

Emergency Access Requests

Test case

- Support to create a ticket for a developer
- Support agent to approve the ticket and to add the developer to the customer group in the Identity and Access Management System
- Check after two days for timer alert
- Further processing of the ticket

Test case

- End user-1 to create a ticket for herself
- Support agent to approve it
- After two days end user-1 informs that the access needs to be extended
- Support to process it
- Check timer alerts

Test case

- End user-2 to create a ticket on behalf of for a developer(requester)
- Support to approve the ticket and to add the developer to the customer group in the Identity and Access Management System
- Check after two days for timer alert
- Further processing of the ticket

5.5.1.1 Findings

As a result of the phase-1 testing, the below issues were found. The root cause for the highlighted issues was also analyzed and they were fixed.

No.	FINDINGS	ROOT CAUSE
1	Agents are unable to select an approver for a ticket	Rights for agent groups in Jira were incorrect
2	The end user is unable to reopen a ticket from portal	The reopening was not correctly defined. Adding a comment in the portal should have reopened the ticket.
3	Queue “Permanent access requests” has all the tickets	Queue incorrectly defined.
4	Too many notifications for end users about requests	Notification scheme for whole Access request project was set up so that the user received notifications also for “In progress” and “Waiting for approval”
5	All agents (Support and IIT) receive notifications of all new tickets	Notification settings
6	The time for opening tickets is not correct (time is off by two hours)	Jira system time is in the wrong time zone. The system time is set on the Jira instance level – not for projects separately.

Table 5.1 Findings and the root cause of testing phase-1

5.5.2 Phase 2

After testing the access request process and ensuring that it is working as per the requirements the next phase was to do the changes for existing users. The access for users who were included in the system after the review process was tested. In the old situation, there was an organization-support group in the Identity and Access Management System where most of the users were added and almost all applications were assigned to that group. Due to these settings, all added users were able to access all applications assigned to that group. These applications include customer environments and internal applications. As per the new access control process, the access should be restricted, and only authorized users should be able to access both the customer environments and internal applications.

Testing was done by selecting the first 20 users whose name start with ‘A' and their access rights were changed in the Identity and access management system as per the new settings. The users were removed from the old organization-support group and were added to specific customer groups. These users were then asked to access their customer environments and application to verify that the process is working fine.

5.5.2.1 Findings

All 20 users, when tried to log in through the Identity and access management system, were not able to access the customer environments. Through detailed investigation and analysis by the access management team, the root cause of the issue was identified. The issue was related to the passing of roles to customer environments when a user login through the Identity and Access Management System.

In the old settings, the SAML configurations on the Identity and Access Management System for each customer environment was done in a way that the organization-support role and all other roles starting with organization-support were passed to the target customer environment for users while they are being authenticated. These roles give varying level of access rights to users in the customer environments. The organization-support role is a default role for all organization employees and the role is needed for users who work on customer projects. This role basically grants the needed permissions to the users to use the service. Similarly, other more specific roles can be created and passed for the user while they are being authenticated by the Identity and Access Management System to implement more granular access control.

During testing, the general availability of organization-support role was disabled by removing all employees from the organization-support group in the Identity and Access Management System. Consequently, there was a need to cut the tie from the role user has to those sent to the customer environments for organization-support. The new SAML configurations for the Identity and Access Management System for each customer environment was done. The previously fixed organization role attribute was moved from Group Attribute Statements to Attribute Statements. Due to these settings, the users who are authorized to access customer environments as per the rules in the Identity access management system, always get the organization-support role when they are authenticated for customer environments.

5.5.3 Phase 3

In the third and last phase of the testing process, first, the issue found in phase 2 regarding the Identity and Access Management System was fixed. The environments were categorized into three types i.e. internal, customer test and all other customer

environments (production, demo, and analysis.). The new settings were first done through a script in three step process for environments. After each step it was tested and verified by test users to ensure it was working correctly. In the first step, the change was done only for the internal environments such as training and simulation environments which do not contain critical customer data. After successful changes for internal environments, the change was done for customer test environments. At last, the new configuration change was applied for rest of customer environments and verification was done by test users.

Fixing the SAML configuration issue in the Identity and Access Management System was followed by again testing the whole access process for the selected group of users. The selected users were removed from organization-support groups and assigned to their relevant customer groups. These users then tried to access the customer environments both for which they are authorized and others for which they are unauthorized. The results of the testing process were as required, and the process was working fine. Later, the new access request process went into production and is being used in the organization for requesting and managing access. Moreover, access logs have already been generated.

5.6 Access Request Analysis

A brief analysis of Jira access requests is done using JQL which is a Jira specific query language. The time span for the analysis is around two weeks. The total number of access requests that are generated since the process went into production is 131. Most of these are permanent access requests as most users are working on customer projects and need access to complete their tasks. So far, 93% of the permanent access requests are created for granting of access and around 2% for revoking of access. Only 4% of emergency requests were generated as it is mainly required to work on customer incidents which do not occur quite often. As there are dedicated service agents who work to manage access requests, the processing time is kept as less as possible. Therefore, only 1% of the access requests are in open status and 4% have already been assigned to the approvers but waiting for the approval.

6 Conclusion

The project was done in collaboration with an organization that is a SaaS provider. The organization deals with a lot of customer confidential data and internal systems to provide customer services and manage operations. As the organization is growing at a fast pace, the existing access mechanisms are not enough to meet industry standards and customer requirements. Therefore, improvement in the existing access control processes was required to meet the growing needs.

The new access control process has been designed to follow standardized security framework best practices while keeping in view both the business and growing organizational needs. The systems in scope were customer environments which are single tenant instances of software that contain the customer-specific confidential data and internal systems that include internally developed as well as third party applications that help the organization to operate effectively. These systems vary a lot in terms of the different organizational roles interacting with them and the sensitivity of data they contain. Therefore, two different approaches were used to cater to the needs of these systems.

The access control process has been designed mainly based on role-based access control model (RBAC). The principles of segregation of duties and least privilege have also been implemented using RBAC. Moreover, the " need to know" principle have been used in some areas. The initial step in implementing an access process based on RBAC is role creation. The roles were created based on the organizational structure and requirements. These roles were then grouped together on the basis of hierarchical structure and requirements of work. Further the access rights and permissions were assigned to these groups. All the users, roles and groups are managed in the Identity and Access Management System.

The access to customer environments was designed based on the role-based access control model. It was categorized into permanent and emergency access based on the purpose and time span for which access is required. The permanent access is granted based on

"roles" to users that are part of the customer project team whereas emergency access is based on "need to know" principle and granted for a short period of time to work on customer issues in case of customer incidents. By default, user are granted the least privilege to customer environments that is managed by sending the user role from the Identity and Access Management System to customer environments while the user is being authenticated. This ensures that user has the minimum privilege in the system. Moreover, varying level of access can be granted based on the role in the same manner.

Access to Internal systems has been defined to be of three different types as per organizational requirement. The first category of systems is preapproved for all employees which means everyone has access to them. The second category includes systems that are only preapproved for specific teams as required by their role. The access to third category of systems can be requested based on the need. The process to manage privileged access to systems is also in place.

Before switching to the new process, it is required to include the existing users in the system. As existing processes were in use, so users already had access to the systems. A review process was conducted for such users. Users were granted access by assigning them to the new roles and groups defined. Those who should not have access were notified and their access was revoked.

In order to enable users to request access to above systems the access request workflows have been designed and implemented in Jira. All users can request any type of access through Jira access request portal by providing the needed information. Each request created in Jira goes through the process of verification and approval by the assigned approvers of a particular system. The segregation of duties is ensured in this process to avoid any conflict. Moreover, the processes to manage, log and track access also exist in Jira which are necessary for reviewing and auditing.

Furthermore, as the new access control process is based on ‘roles’, the change of status process has been implemented to manage the changes in user information that effects the user role and associated access rights. This allows keeping the user profiles updated in

systems such as the Identity and Access Management System and Human Resource Management System, that are involved in the access control process.

The above processes cover all the requirements from SOC 2 and ISO 27001 regarding access control. All controls have been designed, implemented and tested. The organization has a new access control process in place that is compliant with the security standards and helps to manage, verify, log and review access. The organization is not only able to prevent security breaches but also meet the regional and worldwide regulations. The overall process is applicable to any organization that wants to have an access control process in place which is up to industry standards and best practices.

7 References

Atlassian, Working with workflows. Retrieved March 17, 2019, from https://confluence.atlassian.com/adminjiraserver072/working-with-workflows-828787890.html

Clinch, J. (2009). ITIL V3 and Information Security. Retrieved on February 23, 2019 from http://www.noja.co.uk/itilv3_and_information_security_white_paper_may09.pdf

Coyne, E. J. 1995. Role Engineering. *In: Proc. of the 1st ACM Workshop on Role-based Access Control*, article no. 4. Gaithersburg, Maryland, USA.

Craig A., Horne, C. A., Maynard, S. B., & Atif, A. (2017). Information Security Strategy in Organisations: Review, Discussion and Future Research Directions. *Australasian Journal of Information Systems*, Adelaide, Australia.

Denning, D. E., (1976). A Lattice Model of Secure Information Flow. *Communication of the ACM* 19(5), 236-243.

Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (2018). AICPA TSP 100. Retrieved February 12, 2019 from https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/dc-200.pdf

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, p. 92-100.

Ferraiolo, D. F., Cugini, A. J., & Kuhn, D. R. (1995). Role Based Access Control: Features and Motivations. National Institute of Standards and Technology. *In: Proc. of 11th Annual Computer Security Applications Conference*, p. 241-248, Gaithersburg, USA.

Ferraiolo, D. F., Feldman, L. B., & Witte, G. A. (2016). Exploring the next generation of access control methodologies. National Institute of Standards and Technology, *ITIL Bulletin*, SP 800-178. Retrieved from https://pdfs.semanticscholar.org/14bb/aac5363b9516898fa8996133ccf3e4e8c299.pdf?_ga=2.138402549.417639345.1559510095-1457890437.1553456357

Frank, M., Buhman, M. J., & David, B. (2010). On the definition of role mining. *In: Proc. of 15th ACM Symposium on Access Control Models and Technologies*, p. 35-44, Pittsburgh, Pennsylvania, USA. https://csrc.nist.gov/CSRC/media/Publications/white-paper/2010/12/01/economic-analysis-of-rbac-final-report/final/documents/20101219_RBAC2_Final_Report.pdf

Hu, C. V., Ferraiolo, D. F., & Kuhn, D. R. (2006). Assessment of Access Control Systems. National Institute of Standards and Technology Interagency Report 7316.

Retrieved March 5, 2019 from https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7316.pdf

Hu, V. C., & Scarfone, K., (2012) Guidelines for Access Control System Evaluation Metrics. National Institute of Standards and Technology Internal Report 7874. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7874.pdf

Information Technology Infrastructure Library (2011). Service Operations-Best Management Practice. Retrieved on February 29, 2019 from http://www.kornev-online.net/ITIL/04%20-%20ITIL%20V3%202011%20Service%20Operation%20SO.pdf

International Organization for Standardization (2005). Information Technology-Security Techniques, Code of Practice for Information Security Management, ISO/IEC 27002. Retrieved on February 19, 2019 from https://www.academia.edu/7993219/Information_technology_Security_techniques_Code_of_practice_for_information_security_management

International Organization for Standardization (2013). Code of practice for information security controls, ISO-27002. Retrieved on February 19, 2019 from https://www.iso27001security.com/html/27002.html

International Organization for Standardization (2013). Information Technology Security Techniques-Information Security Management: Systems Requirements, ISO/IEC 27001. Retrieved on February 19, 2019 from https://www.iso.org/standard/54534.html

Kissel, R. (2013). Glossary of key information security terms. National Institute of Standards and Technology Internal Report 7298, rev.2. Retrieved on January 22, 2019 from https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Kuhn, D. R., Coyne, E. J., & Weil, T. R., (2010) Adding Attributes to Roles Based Access Control. *IEEE Computer* 43(6), p. 79-81.

Lampson, B. W., Xerox Corporation, & Palo Alto (1974). Protection. *In: Proc. of ACM SIGOPS Operating Systems Review*, p. 18-24, New York, USA.

Loomis, R. J., & O'Connor, A. C. (2010). National Institute of Standards and Technology Final Report: Economic Analysis of Role-Based Access Control. Retrieved on March 3, 2019 from

Ma, X., & Li, R. L. (2010). Role Mining Based on Weights. *In: Proc. of the 15th ACM Symposium on Access Control Models and Technologies*, p. 65-74, Pittsburgh, Pennsylvania, USA.

Ma, X., Li, R., Lu, Z., & Wang, W. (2011). Mining constraints in role-based access control. *Mathematical and Computer Modelling*, 55(2-1), p. 87-69.

Ma, X., Ruixuan, L., Zhengding, L., Jianfeng, L., & Dong, M. (2011). Specifying and enforcing the principle of least privilege in role-based access control. *Concurrency and Computation: Practice and Experience*. 23, p. 1313-1331.

Nwafor, C. I., Zavarsky, P., Ruhl, R., & Lindskog, D. (2012). A COBIT and NIST-Based Conceptual Framework for Enterprise User Account Lifecycle Management. *In: Proc. of World Conference on Internet Security*, p.150-157, Alberta, Canada.

Razieh Sheikhpour, N. M. (2012). A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. *Indian Journal of Science and Technology* 5(2).

Sandhu, R., Ferraiolo, D., & Kuhn, R. (2000). The NIST Model for Role-Based Access Control: Towards a Unified Standard. *In: Proc. of the Fifth ACM Workshop on Role-Based Access Control*, p. 47-63, Berlin, Germany.

Sandhu, R., Ranganathan, K., & Zhang, X. (2006). Secure Information Sharing Enabled by Trusted Computing and PEI Models. *In: Proc. of the ACM Symposium on Information, Computer and Communications Security*, p. 2-12, Taipei, Taiwan.

Sandhu, S. R., Coyne, E. J., Hal, L., Feinstein, H. L. & Youman, C. E. (1996). Role-Based Access Control Models. *IEEE Computer*, 29(2), p. 38-47, Los Alamitos, CA, USA.

Schaad, A., Moffet, J. & Jacob, J. (2001). The role-based access control system of a European bank: a case study and discussion. *In: Proc. of the 6th ACM Symposium on Access Control Models and Technology*, p. 3-9, Chantilly, Virginia, USA.

Security and privacy controls for federal information system and organizations (2014). National Institute of Standards and Technology, SP 800-53. Retrieved on March 11, 2019 from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02192014.pdf

Trust Services Criteria Guide for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2017). AICPA TSP 100. Retrieved February 12, 2019 from https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf

Xu, L. (2017). User Access Review and a UAR Supporting Tool for Improving Manual Access Review Process in Enterprise Environment. Master's Thesis, Department of Information Systems, St. Cloud State University.