3-2017

User Access Review and a UAR Supporting Tool for Improving Manual Access Review Process in Enterprise Environment

Liheng Xu
St. Cloud State University, xuli0701@stcloudstate.edu

User Access Review and a UAR Supporting Tool for Improving Manual Access Review Process in Enterprise Environment

by

Liheng Xu

A Thesis

Submitted to the Graduate Faculty

of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree

Master of Science

in Information Assurance

March, 2017

Thesis Committee:
Dennis Guster, Chairperson
Jim Q. Chen
Balasubramanian Kasi

Abstract

User Access Review is a process of re-evaluating the appropriateness of user access to systems or applications. It is a critical step of the user account management life cycle. Companies implement User Access Review processes to ensure that employees are given least privileges to access critical corporate IT systems, and segregation of duties (SoD) are enabled through effective access control to prevent fraud and error. User access review becomes mandatory for corporations that are in scope under federal regulations, industry standards, or compliances. With growing number of employees (users) and IT systems, the process of conducting user access review becomes increasingly complicated and time-consuming. Corporations often find it changeling to meet audit requirements with existing error prone manual review process and are searching for a better solution for delivering quality access review in a timely manner. A database based user access review tool (UAR Supporting Tool) is proposed in this thesis to improve the efficiency and accuracy of the manual review process.

Table of Contents

Chapter Page

List of Figures

Chapter I: Introduction

In 2002, as a reaction to a number of corporate scandals involving ENRON, TYCO, WorldCom and others, the United States Congress passed the Sarbanes-Oxley Act of 2002 (SOX) to mandate financial disclosure from public companies and prevent fraudulent financial activities. The SOX Act contains seven sections which set requirements to address major issues, such as auditor conflicts of interest, boardroom failures, fraudulent banking practices, unreliable financial disclosure, and weak corporate fraud accountability, to prevent the next major financial crisis (Sarbanes-Oxley Act of 2002, 2002).

Section 404 of SOX states: "*Registered accounting firm shall, in the same report, attest to and report on the assessment on the effectiveness of the internal control structure and procedures for financial reporting*" (Sarbanes-Oxley Act of 2002, 2002).

By requiring accounting firms to assess and report on a public company's internal control for financial reporting, it affirms the integrity of the financial reports (Oracle, 2010). Since financial data that are used to generate financial reports are proceeded and stored in company's IT systems, by ensuring the security of these IT systems, companies are able to attest to the integrity of their financial reports.

Along with the SOX Act, government and industry initiatives such as the Gramm-Leach-Bliley (GLB) Act, the Health Insurance Portability and Accountability (HIPAA) Act, European Anti-Fraud (EU-AF), Payment Card Industry Data Security Standard (PCI-DSS), and the second of the Basel Accords (Basel II) also presents a common standpoint on the importance of internal control for prevention of corporate fraud and individual privacy protection (Oracle, 2006). With sensitive information such as healthcare, payroll, credit card payment, employee personal

information, and company trade secrets processed and stored in corporate IT environments, it is critical for companies to implement user account management to prevent unauthorized user access and temperament of these business critical data.

User Access Review (UAR), also known as Account Review or Account Recertification, is a critical step of the user account management. It periodically evaluates user access throughout the entire life cycle of a user account, from the creation to the termination of a user account. It ensures the appropriateness of user account, and discovers opportunities for improving user account management policies and procedures. With a well-defined and documented process, user access review can effectively reduce risk while providing auditable evidence for meeting regulation or compliance requirement.

However, the process of access review involves strict workflow, heavy communications, and granular details. Companies find it very costly and struggle to meet audit requirements. Although there are commercial products available for managing user access review, these products are often costly to acquire, implement, and difficult to customize to meet all the user access review needs of a company. Therefore, the majority of companies still reply on excel-base manual process to full fill user access review requirements (Oracle, 2006). The manual access review process is time-consuming, error prone, and has very limited flexibilities on how reviews can be organized or scoped. Companies are searching for a better solution for delivering quality access review in a cost-effective way, and meeting audit requirement in a timely manner. The proposed UAR Supporting Tool incorporates a relational data-based structure for better solutions in organizing, presenting, and analyzing identity and access information. It is a manual access

review supporting tool designed for improving the efficiency and accuracy of a manual review process.

The rest of the paper is organized as follows: Chapters II gives background on user access review and related IT security concepts. Chapter III discusses the current state of user access review and challenges with manual processes involved in user access review. Chapter IV reviews two access review products to give examples of the level of maturity of commercially available tools in the market today. Chapter V elaborates on the design and implementation of the UAR Supporting Tool and Chapter VI concludes with discussions and future work.

Chapter II: Background

Before the detailed processes and procedures of user access review is discussed, it is important to understand the role of UAR and its related concepts. User access review is a critical step of user account management, and user account management is a major component of access control, and their relationship with the broader concept of security control can be presented with the diagram as shown in Figure 1.

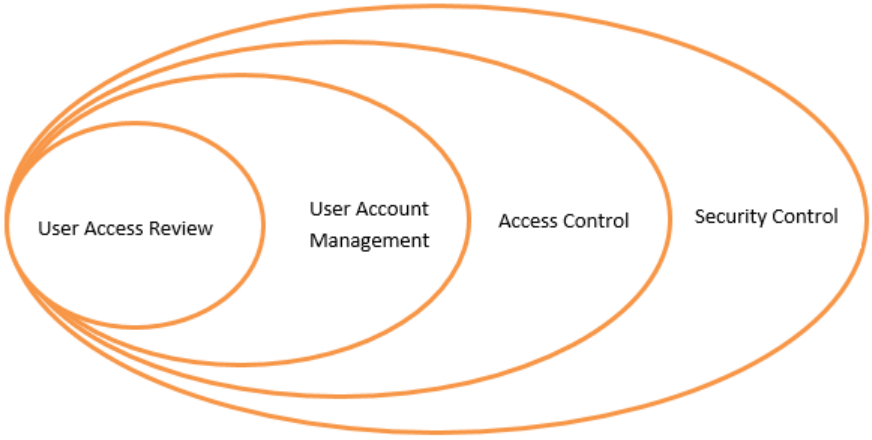


Figure 1. Concept of Security Control

As defined by NIST, security control is "*the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information*" (NIST/ITL, 2004). The three elements of confidentiality, integrity, and availability are commonly referred to as the "CIA Triad" (Figure 2) of information security. Access control as one of the many aspects of security control protects both the "C" (Confidentiality) and "I" (Integrity) of the triad.

Access control includes measures to protect both physical and digital components of an information system. Access to physical locations, such as a server room or a cabin where printed information is stored, can be regulated using locks and keys, whereas user accounts are most

commonly used to control access to digital information, and IT system functions. RBAC is widely used in business environment. It offers many benefits in reducing the cost of access control, but comes with limitations for centralized user access management (Workflow Management Coalition, 1999), and poses difficulty in user access review process. Access control covers the security principle of Separation of Duty, Least Privilege, and many other aspects, and all of these security controls shape the requirements of user account management and user access review.

User account management covers activities of requesting, creation, modification, suspension, termination of user accounts and related access rights. During which, user account management policies are created and the appropriateness of user accounts are defined, procedures, and process are clearly states, and implemented. Although companies set controls in place, it is unsafe to assume that all of the procedures and processes are being followed correctly. User access review serves the auditing purpose in user account management to ensure user access are in-line with company's security policies.

user access review is a critical step of user account management which ensures the appropriateness of user accounts and acts as an auditing function to test the effectiveness of user account management procedures. A high-level view of user access review process includes the follow stages: (a) define policy, (b) gather user access review attestations, and (c) execute and verify remediation.

The sections below discuss access control, user account management, and user access review in details.

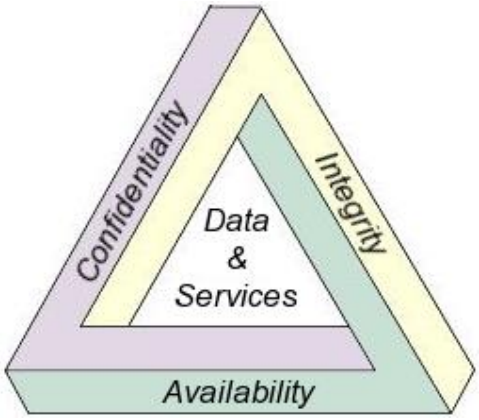


Figure 2. CIA Triad (Ernst & Young, 2013; securitytoolkit, n.d.)

Access Control

NIST defines access control as "the process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances)" (Kissel, 2013). The concept of access control exists long before the modern computer was invented. The phrase was first used in transportation literature in the early 20th Century to describe controlled access roads and highways. Until 1964, the need for access control in the computer system was first described by the MAC Project of MIT to address the issue with data protection in a shared system. According to Joint Task Force Transformation Initiative (National Institute of Standards and Technology [NIST], 2013), access control in term of information security includes to the 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
- Reference monitor

Separation of Duty

Separation of duty (SOD) “addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion” (NIST, 2013). It is “a basic internal control that attempts to ensure no single individual has the authority to execute two or more conflicting sensitive transactions with the potential to impact financial statements” (Ernst & Young, 2010). For example, the personal who receives payments should be different from the person who deposit the payments. There is two major type of SOD, static segregation of duty (SSOD) and dynamic segregation of duty (DSOD).

Static Separation of Duty (SSOD)

SSOD, in comparison to Dynamic SOD, has a predefined set of rules specifying the roles that are conflicting with each other. SSOD prevents system user to be assigned conflicting roles to lower the likelihood of single user conducting fraud. By increase the people involves in the execution of a sensitive business function, the chance of any one user or few users commit fraud is reduced.

Dynamic Separation of Duty (DSOD)

Dynamic separation of duty is a security mechanism that enforces Separation of duty at the time of access. Under this particular method, a user can be granted roles that are conflicting

each other, but only one of these roles can be activated at a time as the user performs related job functions.

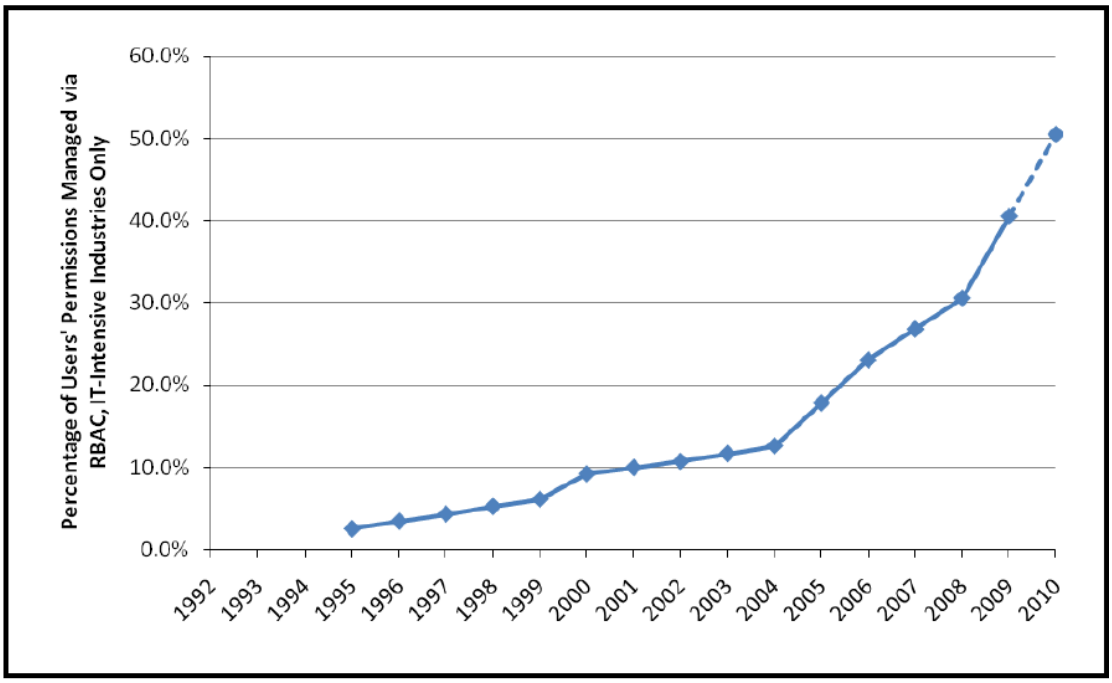
Role Based Access Control

Many access control models have been developed over the years, such as Mandatory Access Control (MAC), Role Based Access Control (RBAC), Discretionary Access Control (DAC), and Rule-Based Access Control (RBAC or RB-RBAC), among which, Role-based access control model is the most widely implemented method in business environment (O'Connor & Loomis, 2010).

Role-Based Access Control (RBAC) was first being referenced by Ferraiolo and Kuhn (1992). Then Sandhu, Coyne, Feinstein, and Youman (1996) published their research defining a family of reference models for RBAC in the effort to categories its application in different systems. According to the NIST guidance (NIST/ITL, 1995), a role is defined as a collection of permissions. Users are assigned roles and acquire the associated permissions defined within the roles. Administrators control access by limiting roles that a user can have. The use of roles to control access is an effective method for enforcing security policies and streamlining the access control process. With the advantage of flexibility and low administrative cost, RBAC was quickly adopted in the field and became the dominant access control model of 1990s.

RBAC is widely used in business environment. As shown in Figure 3, a survey estimated that by the end of 2010, "over 50% of users at organizations with more than 500 employees are expected to have at least some of their permissions managed via roles" (O'Connor & Loomis, 2010). Today, most applications that used by enterprises are developed with built-in role-based access control. Under role-based access control, access rights to applications are first assigned to

roles, users are then assigned the roles needed for completing job tasks. Role-based access control largely reduces user account administration time and cost when compared to user access list where access rights are directly assigned to users.



Note: Industries were defined by 2-digit NAICS code and included utilities; manufacturing; wholesale trade; retail trade; information; finance and insurance; professional, scientific, and technical services; educational services; health care and social assistance; arts, entertainment, and recreation; other services; and public administration.

Figure 3. Percentage of User's Permissions Managed via RBAC (O'Connor & Loomis, 2010)

Limitation of Role Based Access Control

When defining a role, all the permissions a user needs to perform a job function should be neatly encapsulated. Role engineering is the first step of implementing RBAC. During the process of constructing roles, one always has to face the challenge of choosing between strong security and ease administration. Easier administration requires consolidating roles that have similar permissions into one role. Thus, the number of roles will be reduced, as well as the difficulty of access management. On the other hand, strong security requires each role to be more

granular, which might cause multiple roles being assigned per user (Kuhn, Coyne, & Weli, 2010). Companies need to find the balance between strong security and ease of administration during the process of creating roles.

With the increasing number of systems and applications, and the introduction of cloud technology, the IT structure of organizations has become more complex than ever. The RBAC used alone would not be sufficient to provide all the complexity access governance needs a company demands. The RBAC needs to be implemented with rule-based and other more time-tested access method to achieve the most practical value (Hu & Ferraiolo, 2006; NIST/ITL, 2004).

Another limitation of using RBAC is implementing separation of duty controls. Current RBAC products have limited compatibility with SOD controls. Implementing SOD controls using RBAC requires careful design of roles and assign privileges to roles. When assigning privileges to roles, administrators need to make sure the new privileges will not affect existing SOD controls.

User Account Management

User account management also refers to as identity and access management, is a set of policies and procedures or technologies that established for requesting, creating, modifying and terminating user accounts, and related access rights.

Some examples of account management control included in NIST (2013) and O'Connor and Loomis (2013) are:

- Temporary and emergency accounts should be removed or disabled automatically after a predetermined period of time.

- Inactive accounts should be disabled after a predetermined period of time.
- Account creation, modification, enabling, disabling, and removal actions should be automatically audited and reported.
- The organization should require users to log out after a predefined period of inactivity.
- Limit the use of shared/group account credentials, only allow when predefined conditions are met.

Types of Accounts

There are five main categories of information system accounts—user accounts, privilege accounts, shared accounts, system accounts and temporary accounts (Shackleford, 2010). User accounts are accounts assigned to individual users to gain access the IT systems. The privilege accounts are accounts with elevated access rights, such as rights to create user accounts and modify system settings. Shared accounts refer to a single account that is used by multiple users for login. For example, an administrator account is known and used by multiple system administrators to access root privilege in the operating system. System accounts, or service accounts, are used by systems for scheduled jobs, communication to other systems, or act as process owner or application owner. Temporary accounts are accounts used for a one-time instance or a short period of time. Examples of temporary accounts are test accounts, training accounts, or emergency accounts created in case of crisis situations.

User Account Management Life Cycle

Nwafor, Zavarsky, and Ruhl (2012) developed the User Account Lifecycle Management Framework (EUALCMF) aimed to provide companies procedure-level guidelines to implement

recommendations on access control made by the NIST SP 800-53 standard, COBIT 4.1/5 framework and other standards and best practices.

The EUALCMF contains six stages and is repeated at the last stage to form a closed loop of on-going user account management. The six stages are: Policy Definition (PD), Account Requirement (AR), Implement Access (IA), Review Account (RA), Account Termination (AT), and Monitor Account (MA).

As shown in Figure 4, PD is the initial step that defines account management policies, such that defines the purpose, scope, procedures of user account management activities. AR defines an employee's access rights and privileges based on the employee's job responsibilities. IA describes the set of actions needed to create the user accounts with the approved user requirements. RA is the auditing step that ensures current access privileges granted to users are in line with the defined access requirements. The auditing results of any excess rights and accounts are removed from employees in the AT stage. This stage also covers the process of removing access from terminated employees. The MA stage is the continuous monitoring process that targeted to spot any issues that have not yet addressed in the previously defined process which hence leads improvements back to the PD stage described at the beginning to complete the account management circle.

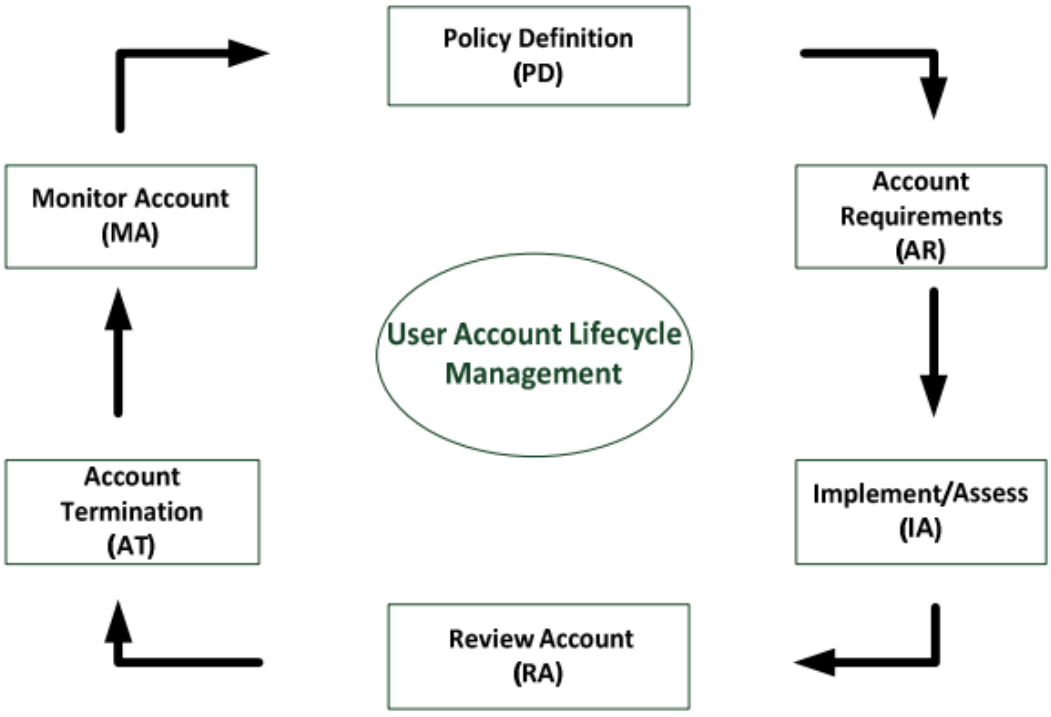


Figure 4. Enterprise User Account Lifecycle Management Framework (Nwafor et al., 2012)

User Access Review (UAR)

User access review evaluates the appropriateness of the access rights that were assigned to a user account, addresses security issues relates excessive privileges and discovers security gaps exist from information security policies. During the process, user accounts are assessed for least privilege, segregation of deities (SOD), and other secure principles and account rules established for preventing fraud and error. A quality user access review not only ensures that user access is in line with user's current job functions, it also uncovers security issues and provides valuable feedbacks on the effectiveness of existing user account management procedures, and system access control policies, therefore, creates opportunities for improvements.

A high-level user access review process. Each organization might implement user access review processes differently, but are all designed around the following fundamental processes of user access review and certification.

Define policy. User access review policies define the goal and scope of user access review, state the required review frequency for reviews, set rules for determining the appropriateness of user access, outline the procedures of access review including the de-provisioning process, and specify the responsibilities of individuals who are involved in the review process.

The scope. It is important to defined the scope before beginning the access review and certification process. With scope properly defined, the review process is reorganized and communicated for effective execution, and guidelines are provided for decision making. The scope of user access review defines which systems are required to be reviewed, and what type of accounts are reviewed. For example, a matured user access review program might include in its scope of all the IT systems within the company, while the other might only include systems that process or contains sensitive information, or systems that are considered at high risk.

The frequency. User access reviews can be grouped into three categories according to the frequency of reviews: trigger based, interval-based, and real- time access review. Trigger-based UAR is initiated by one or multiple pre-defined activities. For example, access review is initiated on all the accounts and privileges owned by an employee, whenever a change in job title information is detected from company's HR system. The trigger-based review is more effective and efficient in a way that reviews are only done as needed. However, with this type of review, there is a risk of not including all trigger events that could possibly pose a security issue when it

relies heavily on the pre-defined rules, which are set up based on existing knowledge and experience. The trigger-based review also required heavily on automated process and tools to support the process, therefore, not every company will have this type of review as an option.

Interval-based access review is the most commonly utilized type of review. The length of Intervals are usually quarterly, semi-annually, and annually. Since the frequency is predetermined, interval-based review validates user access appropriateness at a point of time. In this case, any violation of user account policies occurred in between two intervals will not be detected until the next access review, therefore, the risk is considered to be higher for longer review intervals.

The real-time review is a type of review that provides real –time view of user access information whenever is needed for a reviewer to conduct access review. It is often enabled only with advanced identity and access management (IAM) tool, in which a centralized identity store gets real-time feed on user accounts and access information from all IT systems of within a company. This type of review is the most advanced and automated among all three.

The appropriateness of user account. The appropriateness of user access is usually defined by a company's security policy, which includes requirements from regulation, standards or compliance, as well as company specific requirements on the security of user account. In general, during user access review, accounts are considered appropriate when the least amount of access rights needed for employees to perform their job functions are assigned, at the same time requirements on segregation of duties are met. Other common requirements can include: developers, a software engineer should not be assign access to the production system, an auditor

should be only assigned read-only access, the same employee should not own multiple user accounts within the same system, and etc.

People's responsibilities. Reviewers are the personal exams account and access information and attest to approve and remove user accounts. Typically, they are managers or application owners. Managers have better knowledge of their direct reports, and the job functions they are responsible for, compare to application or system owners, they have less understanding of the system and how the roles and access rights are set up within the system.

Review administrators/internal auditors are personals who manage and coordinate the granular review process, track progress made by reviewers, question attestation results, gather supporting evidence, and are responsible for delivering the access review in a timely manner.

User access review process owner (manager of review administrators) sets procedures for access review, determines review's scope, and access review frequency and schedules. Review administrators are its direct reports.

Auditors (external) assess the result of access reviews to verify regulation and measurement standards are met.

Gather user access review attestations. The access review process starts with generating access report on the current information of user accounts and access rights for systems (per-system) or employees (per-user). When an access report is prepared per- system, it presents all the user accounts with associated account information that currently exists in a system. A per-user report lists out all the system and associated user accounts that an employee currently has access to. Access report captures a point-of-time view of the current state of user

accounts and access rights information for a system. Any changes made after that point of time is irrelevant for analysis until the next round of access review.

In the next step of user access review, access reports are presented to approvers for attestations. Decisions are made for each user account in the report on whether to keep or remove the account and the attached access rights. There are instances that an entire user account needs to be removed, as well as removing partial access rights that are considered excessive form an account, a role or group.

Execute and Verify Remediation

After all the attestations are gathered from the reviewer, review administrators will analyze the access report and attestations to identify any security gaps with company's security policies. Remediation will be executed, during which inappropriate user accounts and access rights are removed, as well as any security issues discovered will be addressed. To verify, a new user access report will be generated to verify whether remediation has been successfully executed.

Chapter III: Current Stage and Challenges

Current Stage

The process of access review involves strict workflow, heavy communications, and granular details. Companies find it very costly and struggle to meet audit requirements. The study shows during 2004, United States companies with exceeding $5 billion spend 0.06% of revenue on SOX compliance, while companies with less than $100 million in revenue spent 2.55% (Figure 5). Access review activities are mostly done manually with spreadsheets today in most corporations (Oracle, 2006).

Companies are seeking for ways to improve their current time consuming, and error prone manual review process. Although there are access review products available in the market that were designed to manage the review process, they are costly to acquire, and implement. Because access review was not required by compliances and regulations until fairly recent, few of the handful review tools that are available in the market is fully developed and has full capacity to automate the entire review process. Companies often find it difficult to find a tool that can be customized to meet all their review needs, and therefore hard to justify to the high cost of acquiring such tool. Therefore, the majority of the companies still have to rely on excel-based manual process to conduct user access review. In consequence, compliances with manual review process are facing variety changelings, and are struggle to meet audit requirements in a timely manner.

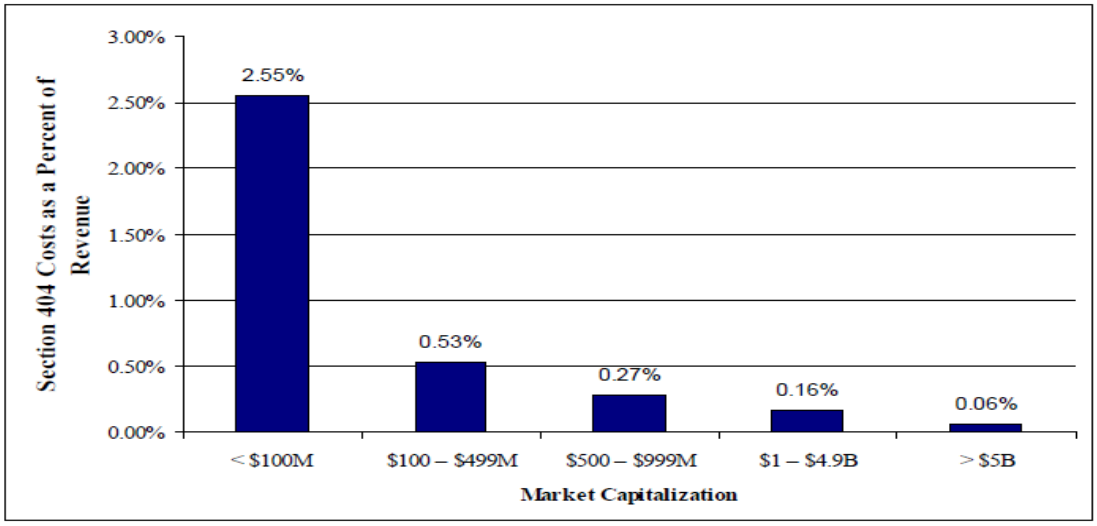


Figure 5. Section 404 Costs as a Percent of Revenue (Smaller Public Companies, 2006)

Challenges

The challenges of manual user access review process are disscussed in the floowing three senctions: detememin last privilege, determemin segergation of duty and data stroage and orgenize.

Determine least privilege. The least privilege control requires that only the minimum amount of access rights are granted to employees for their job duties. To accurately determine what the minimum amount of access rights are for each employee is a complicated and time-consuming task for companies. In order to determine the minimum amount of access rights, it requires knowledge of a user's job duties, as well as how roles, groups, or access rights are defined in systems. Although job functions of a position are often stated in job postings or employee contracts, these documentations present a high-level description and do not contain the details needed for mapping out job functions to information system roles and access rights. Managers often are the people who have the best knowledge of his or her direct reports' job duties. They are able to describe an employee's required tasks in business terms or plain

language but often lack the knowledge of the corresponding roles, groups, or access rights that grant the privileges needed in the system. On the other hand, IT system owners or administrators have the best knowledge of the IT systems they manage but lacks knowledge of an employee's job tasks which determines the minimum amount of access rights required for least privilege. It becomes more complicated to determine least privileges for an employee who needs access to multiple systems, and when systems that have a large number of roles.

Therefore, the first challenge with determining the minimum access is that, without data on employees and systems being collected and managed in a central location, the result would be inaccurate for either the managers or the system owners alone to make the judgments on user accounts.

The second challenge is to keep the data collected on employees and systems up to date in order to reflect the most current job duties of an employee, and roles/access rights exist in a system. Although identity information on employees might not change often, but an employee's job duties change continuously with events such as starting or ending of a projects or programs, being promoted, or moving to a different department. Roles and access rights change from time to time as well, for example, with new roles being created, access rights being added or deleted from roles (change in role definition), or new groups being created. A system or process is needed for capturing these trigger events and record the subsequent changes made in employee job duties, and role definitions, to make sure the data collected is up to date and valid for correctly determine least privileges.

The third challenge is that even with all the data available and kept up to date, it is time-consuming to determine the least privilege for each employee on a case by case basis. A process

is needed for normalize employee and system data and automate the process of mapping employee's job duties to roles and access rights.

Determine segregation of duties. In a manual access review process (access review process without automated UAR tools), segregation of duties is depicted in an Excel-based format call SOD conflict matrix. The SOD conflict matrix is prepared for each system, where roles, groups, or access rights that exist in the system are listed in the first column to the left and first role across the top. Then an X is placed where two roles cross in the matrix to indicate a SOD conflict between the roles. As shown in Figure 6, for the example system, there are varieties task groups that are listed both on the left and top side. When come to determine SOD conflict, Bank Reconciliation task group could not contain the same user as AP Payments groups.

Task Group Description	Grp	1 AP Voucher Entry	2 AP Payments	3 AP Release Blocked Inv	4 AP Clear Vendor Acct.	5 Vendor Mast. Maint. (Acct	6 Vendor Mast. Maint. (Mat)	7 Vendor Mast. Maint. (Ent)	8 Bank Reconciliation	9 AR Cash Application	10 AR Clear Customer Acct.	11 Material Master Maint.	12 Service Master Maint.	13 Requisitioning	14 Release Requisition	14A Process Requisition	15 Purchase Order Entry	16 Purchasing Agreements
AP Voucher Entry	1		X	X	X	X	X	X									X	X
AP Payments	2	X				X	X	X	X								X	X
AP Release Blocked Inv	3	X															X	X
AP Clear Vendor Acct.	4	X															X	
Vendor Mast. Maint. (Acct)	5	X	X				X										X	X
Vendor Mast. Maint. (Mat)	6	X	X			X											X	X
Vendor Mast. Maint. (Ent)	7	X	X														X	X
Bank Reconciliation	8		X							X								
AR Cash Application	9								X									
AR Clear Customer Acct.	10																	
Material Master Maint.	11													X			X	X
Service Master Maint.	12													X			X	X
Requisitioning	13											X	X		X		X	X
Release Requisition	14													X			X	X
Process Requisition	14A													X			X	X

Figure 6. SOD Conflict Matrix (Cincom Control, 2010)

The Excel-based matrix creates challenges for determining SOD conflicts during a manual access review. One reason is that roles that conflict with each other (two-way conflicts) are being recorded twice in the matrix, and the matrix cannot present one-way conflicts correctly. For example, in the above chart, Column 8 Row 2 and Column 2 Row 8 both represent the conflict between Bank Reconciliation group and AP Payments group. However, Column 13 Row 14A shows there is a conflict between Process Requisition group and Requisitioning group, but Column 14A Row 13 indicated requisitioning group and Process requisitions group has no conflict. This is usually caused by roles hierarchy and could easily be overlooked in the SOD conflict matrix. Another reason is that the matrix is difficult to utilize with a manual effort to determine SOD conflicts for all the user accounts listed in a user access report, which is also prepared in an Excel-based file.

Data storage and organization. User access reviews done with a manual process often lack the flexibility to organize reviews in different ways. How reviews can be organized is usually limited to the way data are collected. For example, when Excel-based access report are generated from systems, each report contains a list of accounts that owned by employees that have access to that particular system. Considering a large number of systems and employees a corporation could have, it would be unfeasible with a manual effort to transform these reports to list out all the system accesses each employee owns. Therefore, the data collected based on the system is difficult to be reused for organized user orientated, or other types of access review based on different criteria.

With a manual process, it is a time consuming to identify account owners and correlate to employee identity information, and the results are not always produced with confidence. It is

common for an enterprise level companies to have multiple operating systems, directory services exist in the same IT environment, and applications that have their own authentication methods. Therefore, an employee might be assigned multiple accounts/login IDs for the different types of systems that he or she needs access for. Without a common attribute between these accounts as a unique identifier, it is difficult to determine the ownership of these accounts and correlate to employee identity information.

When user access reports are presented in IT terms, it is difficult for reviewers to use that information to make a judgment on whether the user account is provisioned with appropriate access rights. In a manual review process, access reports are generated directly out of the systems that are being reviewed. The name of roles, access rights, or system objects are usually named with IT terms or abbreviation for convenient development and administration on the IT side. But when they are displayed in access reports, they meant very little to reviewers who are on the business side. For example, a role named "APCLMPMNT" might provide a very little clue to reviewers to find out it grants access for users to posting account payable and claims payments. When access information is presented in a way they cannot interpret, reviewers tend to review only for users based on whether they are still with the company, instead of reviewing the appropriateness of the accounts—which affects the quality of access review and increased the risk of user having more access rights than they needed. Therefore, it is important to provide business-friendly user access report for the best attestation quality.

Chapter IV: Current Access Review Products

There are Access review tools available in the commercial market that will automate or semi-automate the review process. Their maturity in capacity and development varies. Some tools focus on supporting the project management side of user access review. These types of tools provide administrative functions such as distribute user access report by sending out mass emails, automatically sends out email reminders to reviewer, track review progress by calculating the number of accounts that have been attested by reviewers etc. Some tools can take in pre-generated user access report and automatically format the report according to customized requirement, while other tools have connectors that enables them to pull reports directly from different IT systems and director servers. Full automated access review tools have the ability to review and recertify user account and access on predefined conditions and schedules.

To give examples of the capabilities of access review tools that currently available in the market, two tools with different level of maturity are picked and reviewed in the following sections. The two tools are NetIQ Access Review and Oracle Identity Governance.

NetIQ Access Review

NetIQ Access Review is a web-based application that is developed based on general access review practice (Figure 7). This application consists of four stages: Collect, Oversight, Fulfillment, and Reporting.

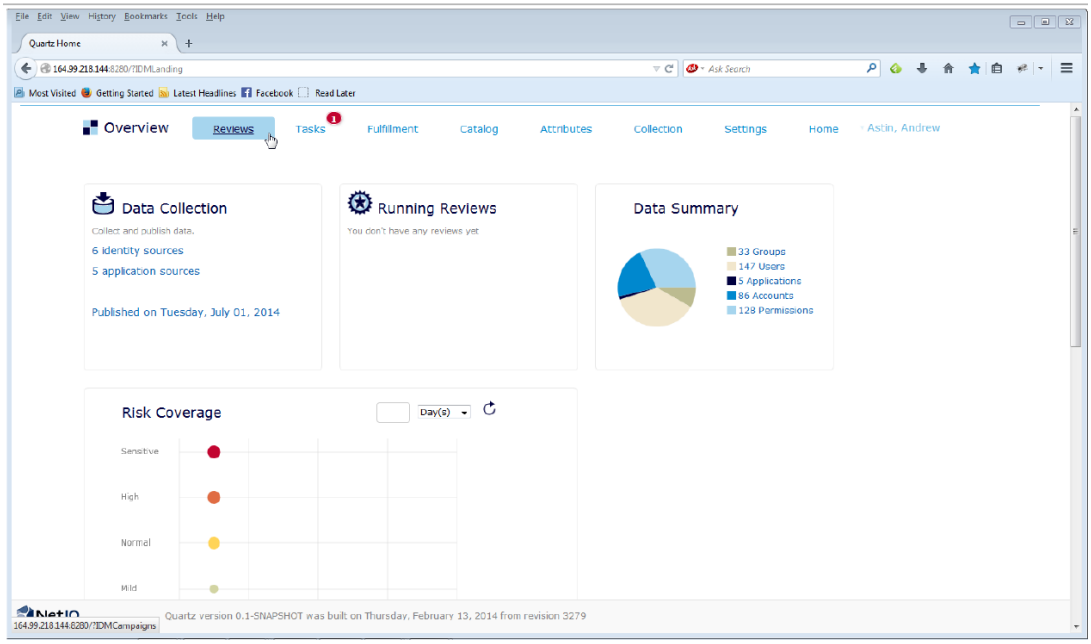


Figure 7. NetIQ Access Review GUI (NetIQ, n.d.)

The Collect stage supports processes of collecting identity information, application information, roles, and user entitlements. All the collected information will be stored in a catalog database where the different types of information are correlated and can be presented in according to different criteria. Access review administrator has the ability to adjust the description of the attributes of the catalog, so that information can be presented in business-friendly context. This application supports NetIQ IDM, CSV file, JAVA database connector (JDBC) and Active Directory as identity source and application source.

The oversight stage defines the scope of user access review. The review scope can be defined by using one or multiple attitudes, such as by the user, group, application, department, job tiles. NetIQ Access Review also offers the ability to setup recurrent access reviews with a timeline view for easy management (Figure 8).

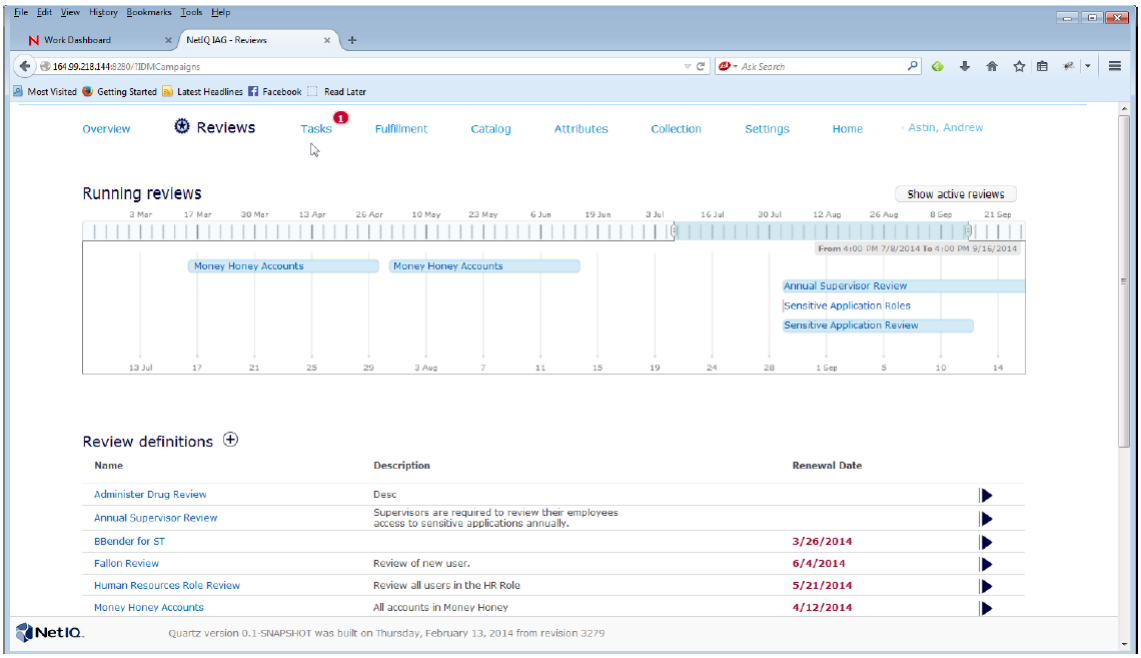


Figure 8. NetIQ Access Review Timeline View GUI (NetIQ, n.d.)

In the Fulfillment Stage, user accounts and access that have been attested to be removed will be removed from employees. In the removal process, this application offers automated revocation through NetIQ IDM, and manual revocation that is monitored through workflow. The revocation will be verified in the subsequent review.

The Reporting Stage provides functions to generate reports for audit testing. External auditors can be given login accounts to NetIQ Access Review which grant auditors access to view the report directly in the application.

The advantage of NetIQ Access Review tool includes a straight forward, and user friendly interface which is easy to use by personals from both business side and IT side. A Running Review Timeline that provides a visualized view for scheduled reviews, and assists review project management. Its catalog database manages attestation information in a central location, and provides an accurate way to correlate user and account information. Compare to

manual process, NetIQ Access Review manages all stage of user access review in one location, which makes over all administration easier.

NetIQ Access Review has couple drawbacks: First, NetIQ Access Review supports only limited number of identity and application sources. NetIQ Access Review depends on these sources to generate a reliable catalog. However, NetIQ Access Review only supports database, Active Directory and .CSV files as source for identity and application information. This makes it difficult for companies to consolidate all of its identity and application information to this review tool. Second, NetIQ Access Review is not a fully automated review tool. The process of evaluating the appropriateness of user accounts and access still relies on manual effort of the reviewers, thus problems such as rubber stamping and review fatigue cannot be avoided by implementing this review tool. This allows opportunities for error and lows the quality of the access reviews.

Oracle Identity Governance Suite

As one of the four components of Oracle Identity and Access Management solution, Oracle Identity Governance suite empower user self-service, simplify audit and compliance task, and automate IT operations. Oracle Identity Governance provides functions like access request and self-service, role lifecycle management, access grants, identity certification, account management and identity audit monitoring and reporting. Among these functions, the identity certification, and identity audit function enables fully automated user access review with scalability and sustainability. This solution has the capabilities to automatically collect, correlate and audit identity data from multiple resources and applications. It enables risk-based access review scoping, and prescheduled reviews for dynamic access reviews. User access reports are

presented to business managers and IT owner with a customized UI (Figure9). This solution also supports automated detection and prevention of policy violations using predefined rules.

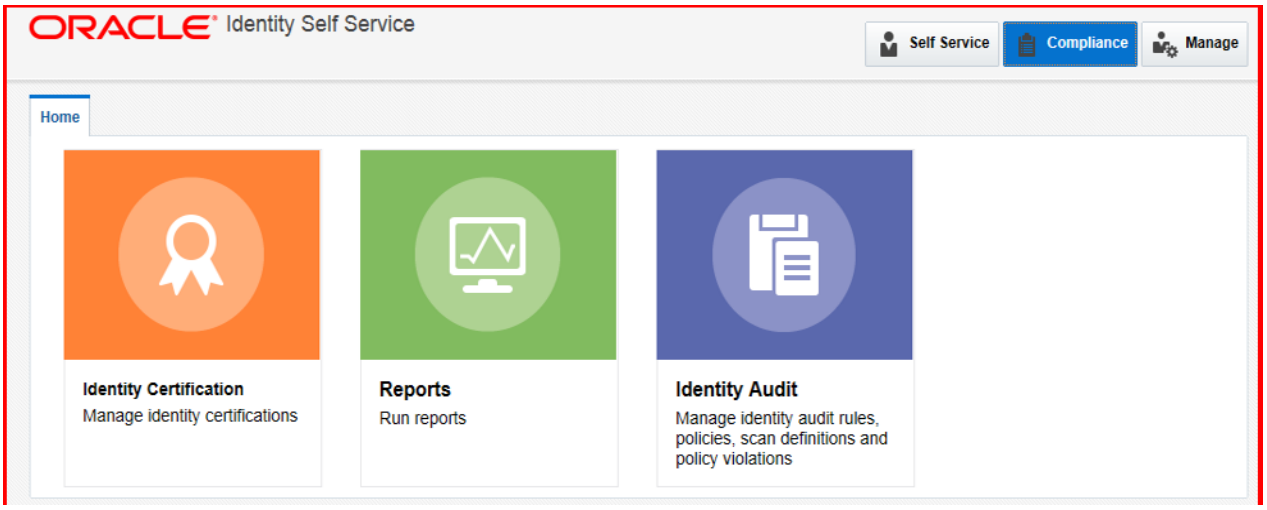


Figure 9. Oracle Identity Governance Suite Customized GUI (Oracle, n.d.)

One of the Oracle Identity Governance suite's key feature is that it uses a "risk-based" review process. As shown in Figure 10, the process starts with collecting data from varieties sources and store them in the identity warehouse. Certification administrator has the abilities to label the risk of each individual objects or groups. Then the identity data will be correlated and aggregated by risk into different categories. The low-risk users will be certified by a traditional approach: business manager review and approve. The high-risk users will be presented to reviewer with a 360-degree view of their access. 360-degree view includes a list of all the access owned by a user, access requests and assignment history, and results of analysis on SOD conflicts and access usage. For example, if a user requested access througth proper procedures by using the access request function in Oracle Identity Governance suite, this user will be tagged for low-risk. In this case, the traditional approach will be used for review on this user. In another case, if a user gains access without a record of request, this user will be tagged for high-risk, and

the 360-degree view will be attached to the review report to provide detailed information to support reviewer decisions.

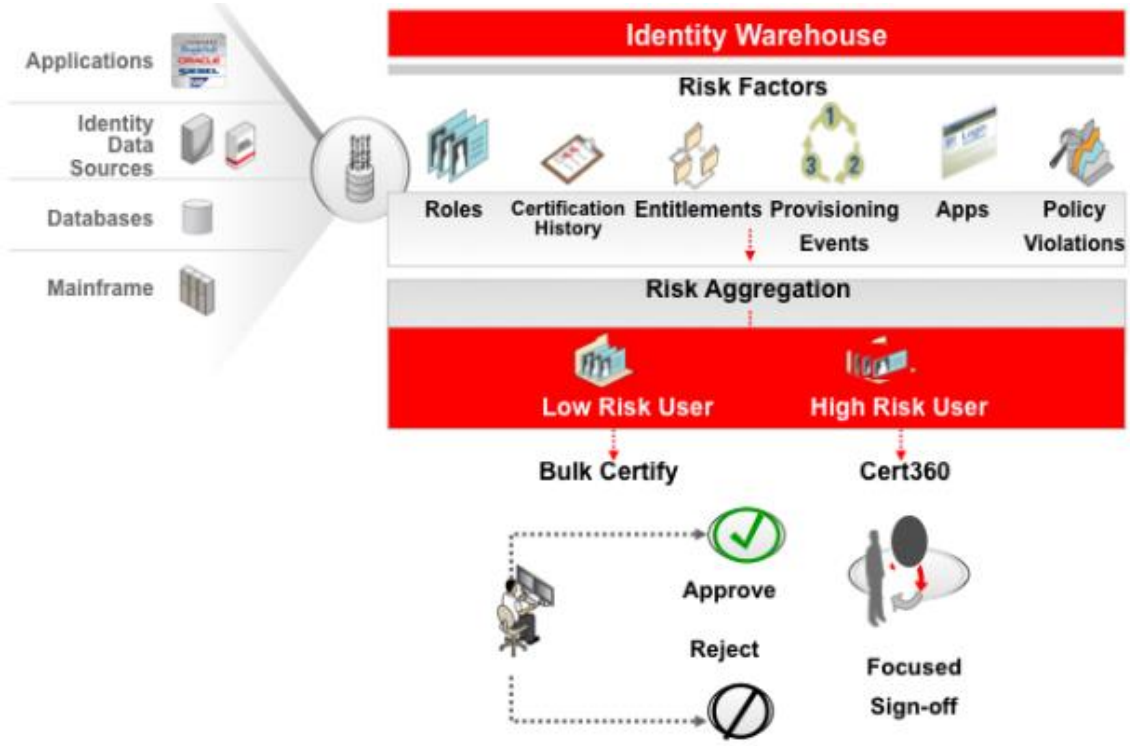


Figure 10. Oracle Identity Governance Process Chart (Oracle, n.d.)

Another key feature provided by Oracle Identity Governance suite is the identity audit function. This function allows automated detection and prevention of policy violations using predefined rules. Internal auditors can setup access rules according to regulations or compliances. Individual rules then are grouped to form policies. By assigning policies to different objects, this function will carry out scheduled detective scan to discover any policy violations and remediate unnecessary access, and run a real-time protective scan to prevent new access that is against the current policy being assigned. All the actions taken by identity audit function during detective and protective scan will be formalized into a report for audit purpose.

Comparing to other access review solutions, Oracle Identity Governance Suite provides a fully automated access review process and supports wide ranges of applications as its identity resource. The fully automate identity audit function helps companies to reduce the risk of rogue access and provide real-time application of security policies. This solution also supports majority of the applications currently available in the market as its data source. Together with other functions provided by Oracle Identity Governance forms a complete solution to companies' identity governance need. The only drawback of this solution is the cost to acquire and implement in companies' IT environment.

Chapter V: User Access Review (UAR) Supporting Tool

As described in the pervious chapter, there are user access review tools available in the market today that can help with challenges found during the manual review process. But the majority choose to reply on the manual effort to complete the review process. User access review is a fairly new process, there are very few options when comes to choosing an UAR tool. Since there are few suppliers in the market, UAR tools are costly to acquire, implement, and not always able to be tailored to meet all of a company's review needs. Fully automated UAR tools usually only come as an add-on to advance IAM software. Companies that are not ready for an automated IAM and UAR tool at the current stage, are in searching for methods to improve their manual process to be more sufficient and effective.

A large portion of the user access review process is around organizing, presenting, and analyzing identity and access information, and these are also the areas in which companies found difficult to manage with current Excel-based manual process. A different method for organizing, presenting, and analyzing identity and access information is needed in order to improve the review process. A relational database should be used for this purpose. A relational database provides a superior data structure for organizing, presenting, and analyzing identity and access information, and has the capacity to solve the challenges found with excel- base manual review process.

The UAR Support tool is an MS Access based design that supports access review process, improves the accuracy, effectiveness, and efficiency of the manual activities involved. Discussed in the previous chapter, these are the challenges that faced by companies that adopt a manual review process:

1. Access reports generated from each system are stored in separate documents with different file formats.
2. Difficult to correlate user accounts existed in different systems to employee identity
3. Lack of accuracy in providing reviewers account owner identity information such as department, job title, employment status or term dates for contractors, and manager name.
4. Role name, group name, access right, and other account details that presented to reviewers are in technical terms or abbreviations.
5. User accounts and access information generated from each system take unrealistic amount of manual effect to be organized into a different view other than "by system."

The UAR Support tool solves above challenges by enables functions to:

1. Organize review data (e.g. access reports, system reference, SOD matrix) for all systems at a central location.
2. Provide flexibility to export access report and scope/organize reviews based on multiple criteria.
3. Translates IT terms and abbreviation into business-friendly language for better review quality.
4. Automatically correlates user accounts to employee identity information.
5. Provides a form view for collecting attestation Information, which eliminates the time-consuming manual process to consolidate attestations from different reviewers into one spreadsheet.

The UAR Support tool is designed with MS Access database. Although MS Access lacks many functions, and scalability when comparing to more advanced dataset system such as Oracle DB, and SQL Server, it is the best option for the purpose of the UAR Support tool, which is to support manual access review process. MS Access database comes with the MS office suite and is ready for companies to use without occurring additional investment cost. Its graphical interface, guided macro creation, and intergraded form design make MS Access easy to adopt by personals from both business and IT side. It also supports sharing through split database function, network folder, SharePoint site, or database server. The table relationship of the UAR Support tool can be used as a reference for implementation in database software other than MS Access.

Initial Set-up

Collect and import review related data. Employee Table-Employee identity information should be collected from human resource database and import into a linked table in the database for automatic updates. Employee identity information should be kept current as it provides information on employee name, LanID (local network ID, which is a key employee identifier in user accounts), employment status (ex. active/termed), employee current job title, department, business segment, and manager name, etc. This employee identity information is critical in the process of determining the appropriateness of user accounts.

System Table-System related information should be collected from multiple sources, such as IT system repository, system owners, and administrators. System information includes, for example, system name, system repository ID, system description, business segment, system

business owner (data owner), system IT owner, system type (application, database, server, Share drive etc.), platform/OS, and Compliance Scope (SOX, PCI, SSAE16, etc.)

Permission, Permission_Objects, Objects Table-Role, group, access level, access rights, and system objects information should be collected for each system. The Permission_Objects table lists out, for example, all the access rights on objects that are permitted by a Role.

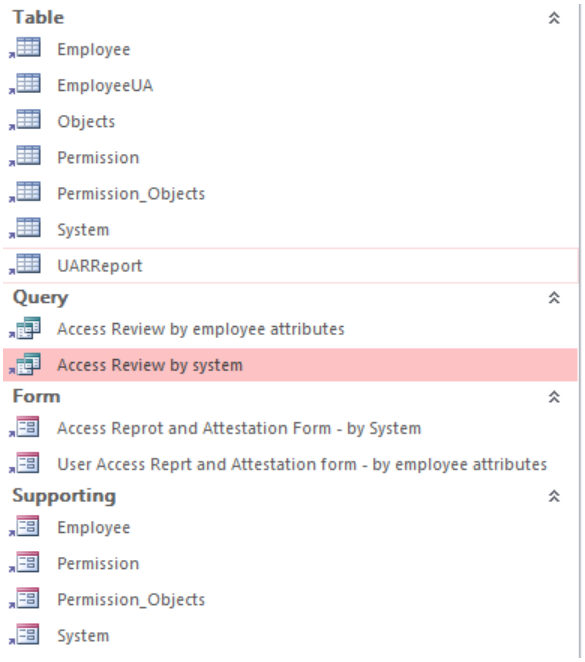


Figure 11. Database Structure Chart

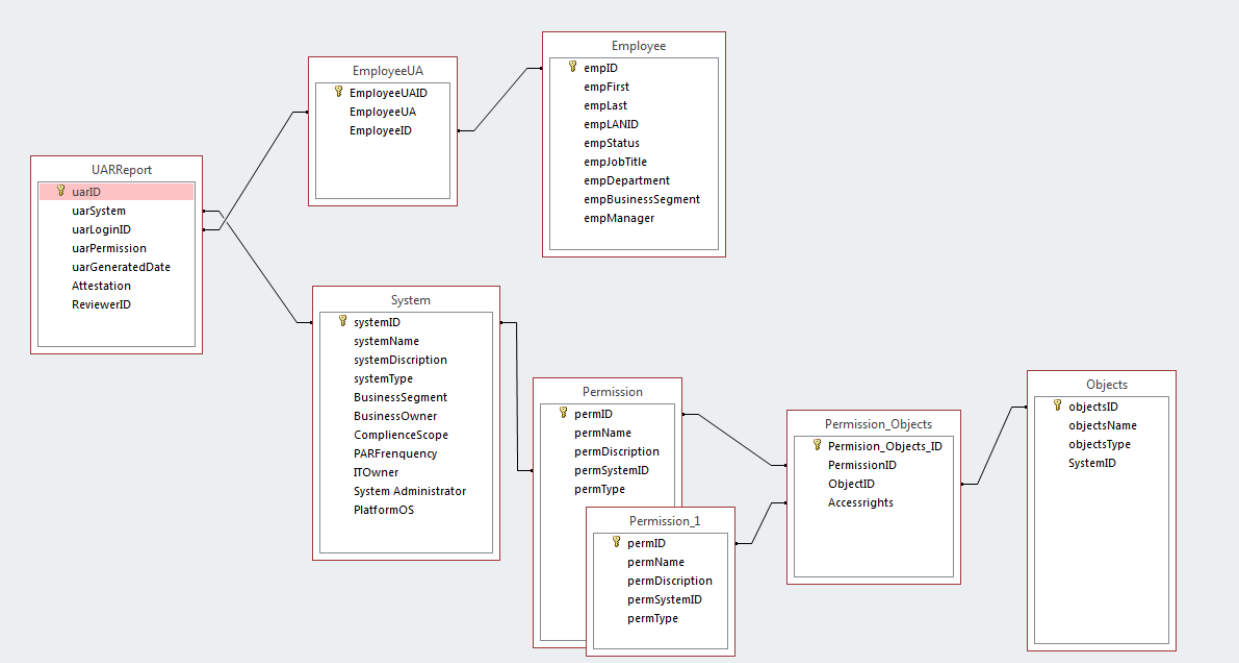


Figure 12. Database Relation Chart

Share between multiple users. During the review process, reviewers such as employees' direct manager, or system administrator will need access to the database in order to put in their attestations/certifications on user accounts. It is important that during the initial set-up, proper sharing methods should be decided on. The diagram below lists out factors to considerate for picking an MS access DB sharing methods. Companies should decide by estimate how many reviewers will be accessing the DB at the same time, and evaluate other factors data availability and performs.

Factors to consider

	Split database	Network folder	SharePoint site	Database server
Requires database server software?	N	N	N	Y
Requires Windows Server 2003 or later?	N	N	Y	N
Data availability	Good	Adequate for small groups with light data-editing	Best	Best
Security	Depends on additional measures	Least secure method	Best	Best
Flexibility	Flexible. Can easily develop new database features without disrupting work. Each user can modify the design of objects in her own copy.	Less flexible. Development can be done with offline copy of database, which is then replaced. Does not allow users to individually modify database design.	Flexible. Depends on method of sharing. With publishing, can control which forms and reports are available. With linking, users can modify their own copies of the database.	Flexible. Can easily develop new database features without disrupting work. Each user can modify the design of objects in her own copy.

Figure 13. Ways to Share an Access Database (Microsoft, n.d.)

Workflow

- Generate user access report form systems
- Import user access report into the UARReport table.
- Use the *Access Review by system* query (Figure 14) to filter on reviews by system, or use the *Access Review by employee attributes* query (Figure 15) to organize reviews specifying any criteria on employees (ex. by IT department, by manager, by job title)

```
SELECT UARReport.uarID, UARReport.uarSystem, UARReport.uarLoginID, UARReport.uarPermission, UARReport.uarGeneratedDate,
UARReport.Attestation, UARReport.ReviewerID
FROM UARReport
WHERE (((UARReport.uarSystem)=2));
```

Figure 14. Access Review by System Query

```
SELECT Employee.empID, Employee.empFirst, Employee.empLast, Employee.empLANID, Employee.empStatus, Employee.empJobTitle,
Employee.empDepartment, Employee.empBusinessSegment, Employee.empManager, EmployeeUA.EmployeeUA, UARReport.uarSystem,
UARReport.uarPermission, UARReport.uarGeneratedDate, UARReport.Attestation, UARReport.ReviewerID, EmployeeUA.EmployeeID,
UARReport.uarLoginID
FROM UARReport INNER JOIN (Employee INNER JOIN EmployeeUA ON Employee.empID = EmployeeUA.EmployeeID) ON
UARReport.uarLoginID = EmployeeUA.EmployeeUA
WHERE (((Employee.empDepartment)="IT"));
```

Figure 15. Access Review by Employee Attributes

- Open up the *Access Report and Attestation Form—by System* (Figure 16) or the *User Access Report and Attestation form—by employee* (Figure 17) attributes to review user account access.

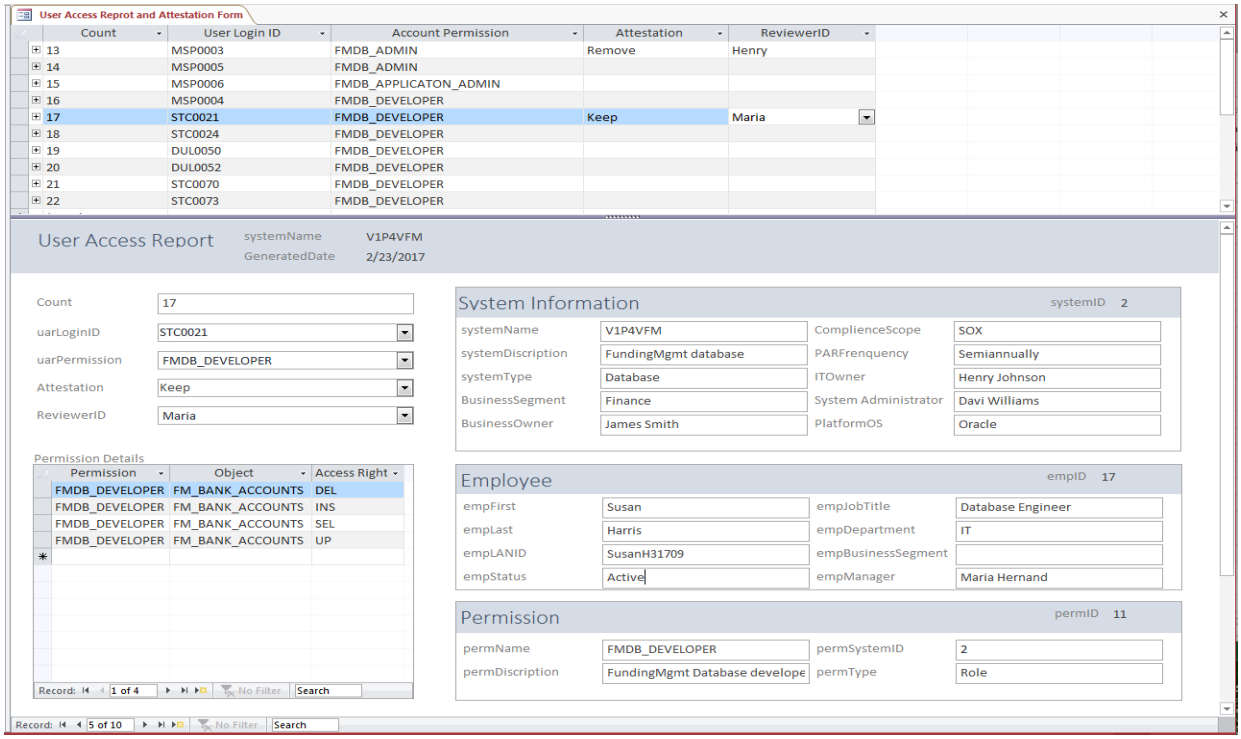


Figure 16. Access Report and Attestation Form—by System

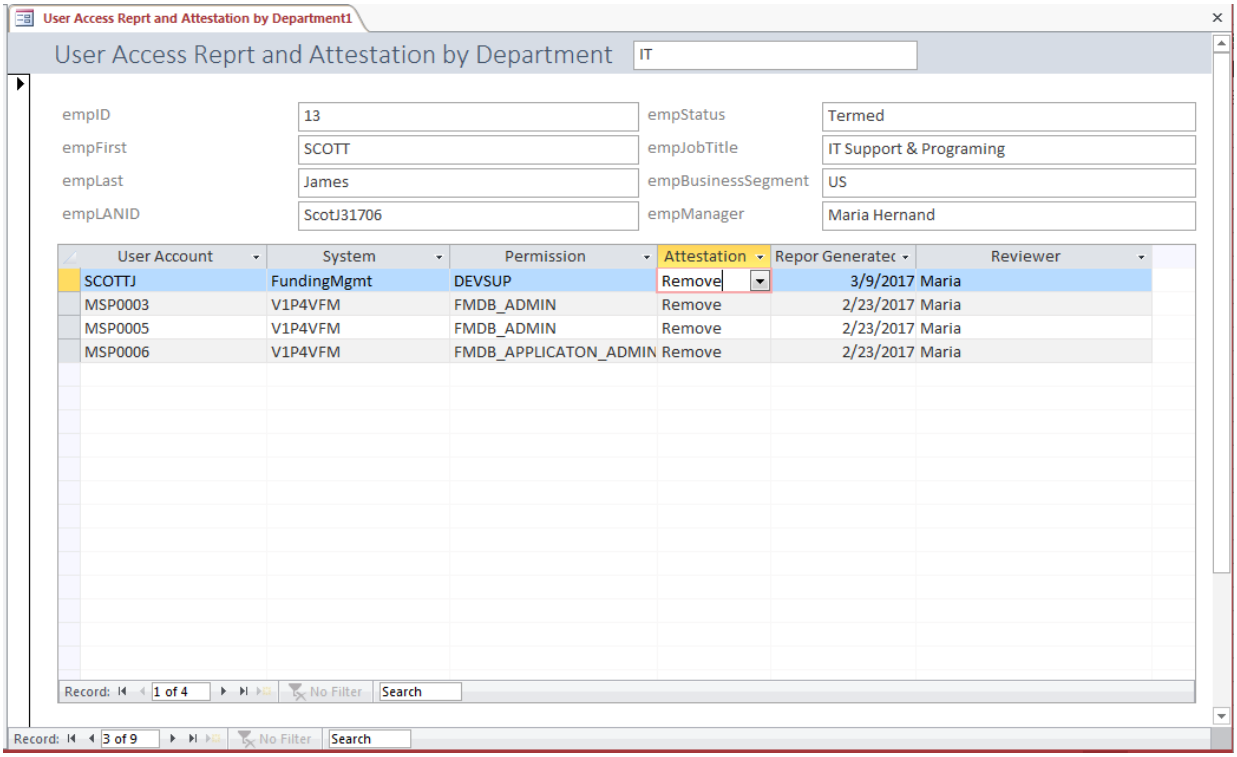


Figure 17. Access Report and Attestation Form—by Employee

Chapter VI: Conclusion

With sensitive information such as financial, healthcare, payroll, credit card payment, employee personal information, and company trade secrets processed and stored in corporate IT environments, it is crucial for companies to implement identity and access management to prevent unauthorized user access and temperament of these business-critical data.

With the emergence of cloud computing services, Identity and access management becomes more important than ever. Cloud computing creates new access control risks and challenges to manage access to sensitive data. Management of a server in the cloud requires elevated accounts. When accounts with elevated access rights are compromised, attackers might be able to intercept sensitive data from, and gain access and control to the most valuable target in the cloud. Thus, user account management must be implemented to manage the user accounts and access to the cloud based applications to lower the risk of undetected data loss, tampering, and resultant fraud.

User access review as a critical step in the user account life cycle management, serves as a detective process for identify inappropriate user accounts, and access to systems and applications. It evaluates the appropriateness of the access rights that were assigned to a user account, addresses security issues relates excessive privileges and discovers security gaps exist from information security policies. As companies grow larger, the number of employees and turnover rates rises, the number of systems and applications in companies' IT environment increases. This makes managing user accounts and access to IT systems and information assets become increasingly complex. As a result, access review becomes more complicated, and the current excel-based manual process becomes insufficient to meet review requirements.

Fully automated user access review tool available today in the market only comes with advanced IAM suit. Advanced IAM products are extremely costly to acquire. Organizations like universities, hospitals, banks and finical institute usually have stronger demands for IAM than companies from for example, manufactory industry caused by these factors: user account turnover rate, the level of risk related data and information stored and processed in IT systems, and how often does the organizations acquire new applications. Therefore, even when there are fully automated IAM tools available in the commercial market today, not all companies can justify to acquiring one based on cost and benefits analysis. As a result, the majority of the companies still rely on manual process to conduct user access review.

The proposed UAR supporting tool built with MS Access database provides solutions to challenges of the current manual process discovered around organizing, presenting, and analyzing identity and access information. This tool organizes review data (e.g., access reports, system reference, SOD matrix) for all systems at a central location, provides flexibility to export access report and scope/organize reviews based on multiple criteria, translates IT terms and abbreviation into business-friendly language for better review quality, automatically correlates user accounts to employee identity information, and provides a form view for collecting attestation Information. With a relational data structure, and user friendly form interface, the UAR supporting tool improves the effectiveness, efficiency, and the accuracy of the manual activities involved in manual review process.

Although the UAR spurting tool presented in the paper does not have the full capacity to replace advanced and fully developed commercial review tools, it serves as an interim tool for companies to use while moving toward an automated solution.

Many of the challenges faced in the current manual access review are the same challenges faced by user account management. Although regulations, standards, and compliances such as the SOX Act, HIPPA, GLBA, and the BASEL II Accord are the primary drive for companies to conduct user access review, companies should not do it to merely meet compliance requirements, neither should they fall back on their user access review process to enforce access control. Instead, companies should realize the business value of and invest in user account management and IAM solutions to evolve from a compliance-orientated user access review to a business-orientated and risk-orientated review program in the future.

References

Cincom Control. (2010). *Cincom Control: Role-based ERP*. Retrieved from http://erp.cincom.com/2010/08/cincom-control-role-based-erp/

Ernst & Young (2010). *A risk-based approch to segregation of duties.* United Kingdom: London.

Ferraiolo, D. & Kuhn, R. (1992). Role-based access control. *Proceedings of the NIST-NSA National Computer Security Conference* (pp. 554-563), Baltimore, MD.

Hu, V. C., & Ferraiolo, D. F. (2006). *Assessment of access control system.* Gaithersburg, MD: NIST.

Kissel, R. (2013). *Glossary of key information security terms.* Gaithersburg, MD: NIST.

Kuhn, D. R., Coyne, E. J., & Weli, T. R. (2010). Adding attributes to role-based access control. *IEEE Computer, 43*(6), 79-81.

Microsoft. (n.d.). *Ways to share an access database.* Retrieved from Microsoft: https://support.office.com/en-us/article/Ways-to-share-an-Access-database-2c24eb08-bee1-453e-be8e-455f847c5c74

National Institute of Standards and Technology. (2013). *Security and privacy controls for federal information system and organizations* (NIST Special Publication 800-53). Gaithersburg, MD: Author.

NetIQ. (n.d.). *Identity governance for access cerification and reducing the risk of excessive access*. Retrieved from NetIQ: https://www.netiq.com/products/identity-governance/

NIST/ITL. (1995). *An introduction to role-based access control*. Retrieved from NIST: http://csrc.nist.gov/rbac/NIST-ITL-RBAC-bulletin.html

NIST/ITL. (2004). *Standards for security categorization of federal information and information systems.* Gaithersburg, MD: NIST.

Nwafor, C. I, Zavarsky, P., & Ruhl, R. (2012). A COBIT and NIST-based conceptual framework for enterprise user account lifecycle management. *World Congress on Internet Securiry*, 150-157.

O'Connor, A. C., & Loomis, R. J. (2010). *2010 economic analysis of role-based access control.* Gaithersburg, MD: NIST.

Oracle. (2006). *Attestation of identity information.* Retrieved from http://www.economist.com/media/oraclecompliance06/6_AchievingSarbane-Oxley.pdf

Oracle. (2010). *Identity and access management: Enabling Sarbanes-Oxley compliance.* Oracle White Paper. Retrieved from http://www.oracle.com/us/products/middleware/identity-management/061145

Oracle. (n.d.). *Oracle identity governance*. Retrieved from Oracle: http://www.oracle.com/us/products/middleware/identity-management/governance/overview/index.html

Sandhu, R. S., Coyne, E. J. Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *IEEE Computer, 29*(2), 38-47.

Sarbanes-Oxley Act of 2002. (2002). *H. R. 3763—107th Congresss: Sarbanes-Oxley Act of 2002*. Retrieved from United State Goverment Publishing Office: https://www.gpo.gov/fdsys/pkg/PLAW-107publ204/html/PLAW-107publ204.htm

securitytoolkit. (n.d.). *A blog for those intereseted in information security*. Retrieved from securitytoolkit: https://securitytoolkit.wordpress.com/

Shackleford, D. (2010). *Keys to the kingdom: Monitoring privileged user actions for security and compliance.* Boston, MA: SANS Institute.

Smaller Public Companies. (2006). *Final report of Advisory Committee on Smaller Public Companies to the U.S. Securities and Exchange Commission.* Washington, DC: Author.

Workflow Management Coalition. (1999). *Workflow management coalition terminology and glossary.* Retrieved from Wolkflow Management Coalition: http://www.wfmc.org