Best Practices, Procedures and Methods for Access Control Management

Michael Haythorn

July 13, 2013

Table of Contents

Abstract

Controlling access to information and information systems is a fundamental responsibility of information security professionals. The basic need to consume data creates a requirement to provide control over the access necessary to use that data. It is this subject-object interaction that introduces risk that must be mitigated through methodological policy creation and enforcement. Access controls are managed through the provision of rules to grant/deny subjects who intend to access certain objects. These rules can be defined and enforced through a number of means to create a manageable layered control process. The overarching goal of access control is to facilitate the mitigation of risk to the object.

In order to access data, multiple layers must be passed through including identification, authentication, and authorization. Actions of subjects must be monitored, creating accountability. Depending on the requirement for policy enforcement and level of sensitivity of the data to be protected, there are multiple methods that can be implemented to control access. The principle of least privilege, separation of duties, job rotation, mandatory access control, discretionary access control, role based access control and rule based access controls are most commonly used.

In addition, industry standards have been established both by government and private entities to identify best practices. ISO/IEC 27002 standard outlines the management of access control policy and enforcement. The government created standard NIST 800-53 and 800-53(A) identifies methods to control access by utilizing various models depending on the circumstances of the need.

1 What is Access?

The necessity of control is created by the need for access. Access is essentially the ability of the subject and the object to interact. In the terms for this paper, all access is logical, meaning that it exists on a system and is typically a file, folder, program, system or process. The request for access is initiated by the subject and is necessary in all information systems circumstances.

1.1 Access Control

Access control is essential where there is sensitive data to protect or privileged actions to be performed. In order to control the use of these functions, there must be a way to limit access. Without this control there would be no ability to prevent unauthorized access to privileged data inside a system. Imagine if any employee working for a soft drink company were able to see the secret formula or if all employees working for large private financial company were able to see the salary of their coworkers. These situations would cause company collapse or employee mutiny because not all data is intended for everyone.

Thankfully there is access control in place to prevent the situations above. By using the proper means to control who accesses data, along with when and where it is accessible this data can be protected in order to maintain a competitive advantage, or establish a level of division required for an entity to survive.

1.2 Identification

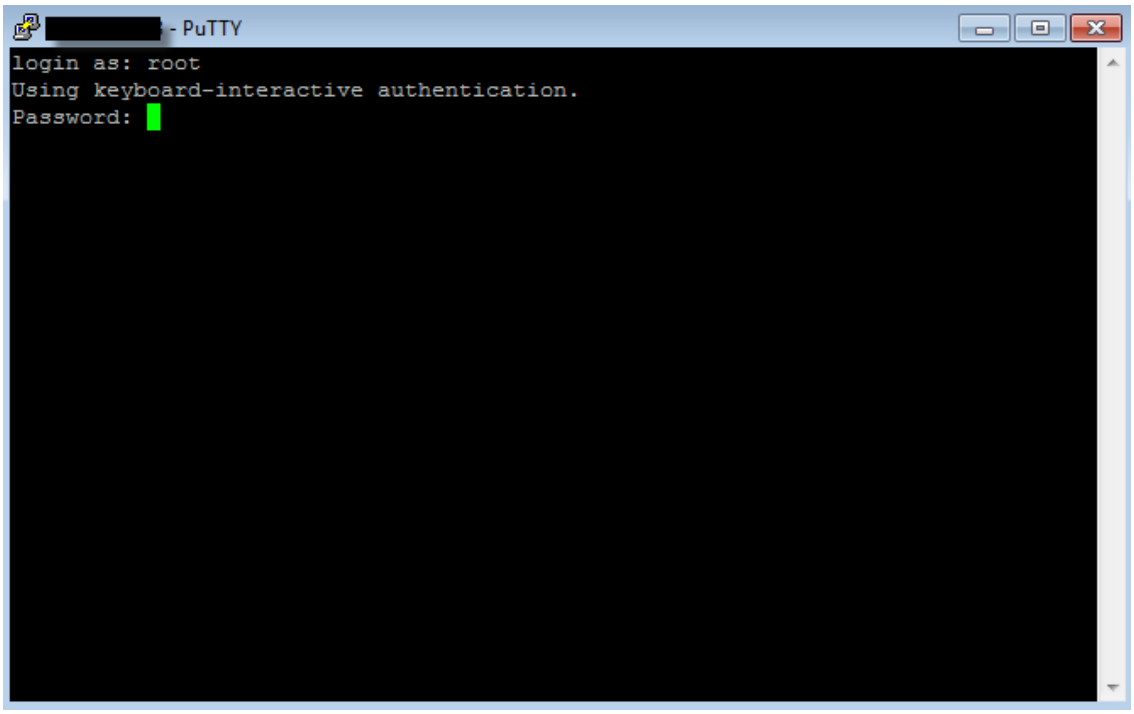
Identification describes a method of ensuring that the subject is in fact who they claim to be. An identity can be assigned to a user a user, program, or process and is used by the system to associate the subject with the identity stored on the system. An example of identification is a user name for a user who is accessing a desktop through a log in screen. In this case the user name is unique to that user and is required for access to be granted. For the purpose of accessing a system or process, the identifier does not need to be unique to a user, but can be generic. The only requirement is that this identity be linked to the process or program on the system so that it can be identified.

Diagram 1.1 shows a typical identification request where the system is asking the subject to provide a user name that it will use to associate with a profile stored on the system:

1.3 Authentication

Identification is half of the typical login process. The next step is authentication where a user, program or process must provide some type of password, passphrase, token, biometric, or key that is matched to the user name and matched to the credential stored on the system or on the network that is being accessed. Once authentication is passed, access is granted or denied to the system based on the information provided. For example, a UNIX user provides a user name and password to log into a UNIX system. The user is only authenticated at this stage yet still does not have access to perform and functions on the system.

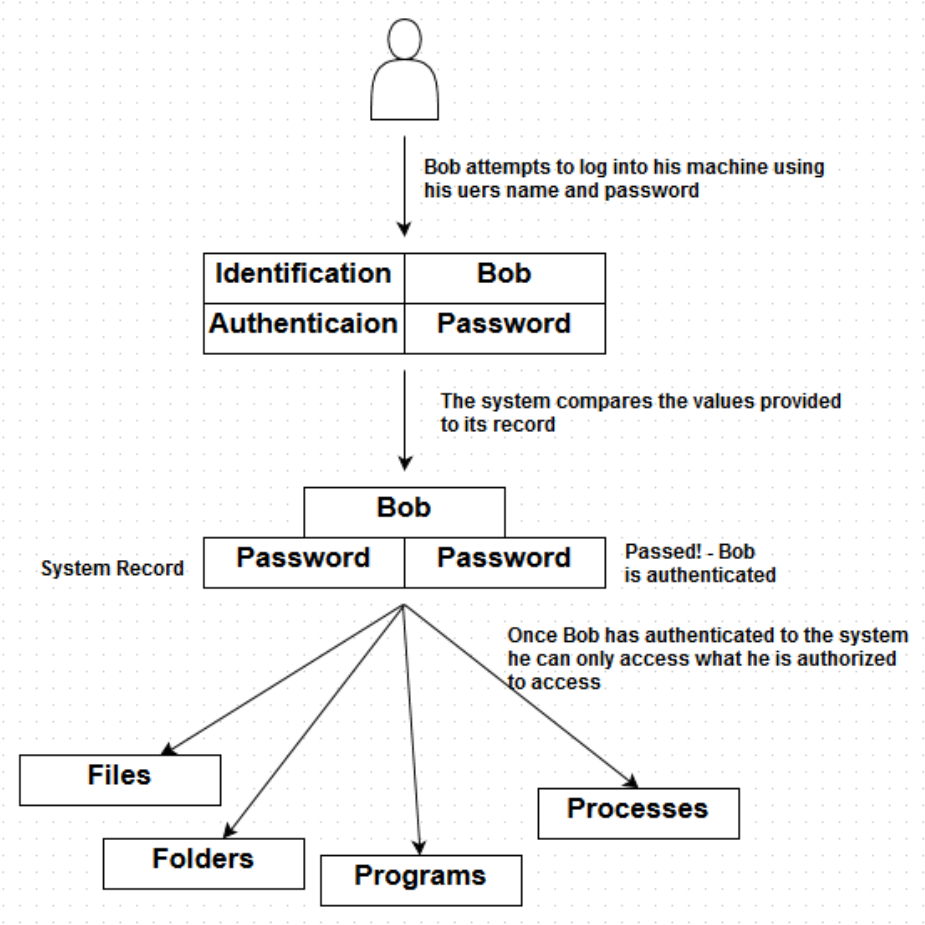
Diagram 1.2 shows a typical authentication request on a UNIX System where once the user name "root" is provided the system requests the password that is associated with the identifier:



1.4 Authorization

The next piece is the authorization of access that is granted to that user, program or process. This control either allows or denies action based on rules that are defined inside the system pertaining to that subject. Rules are defined in many ways and can be based on request, time, location, group, etc. An example of authorization is a subject requesting access to a network shared drive. In this example the subject has successfully identified themselves and authenticated to the system. Their attempt to connect to the shared drive must also be authorized by some control that will grant them this additional access. If the user is granted the access they will be able to connect to the shared drive. If the user does not have the necessary authorization to connect they will be denied access. Authorization is where access control is established and can be implemented at both the macro and micro level depending on the sensitivity of the data and the policy being enforced.

Diagram 1.2 displays the process of identification, authentication and authorization through the use of a flow chart that can grant or deny access based on the information given and the rules it has been supplied:



1.5 Accountability

Finally in order to enforce the misuse of policy once access has been granted, or prevent repeated malicious access attempts there must be some form of accountability. Accountability can use various methods to record or capture events for additional review. This event log can include every access request, both positive and negative, subject login times and locations, subject actions upon login, etc. This information is stored and can be used for investigative purposes or for reporting of usage statistics for audit. Accountability is essential to be able to provide proof of action and without this piece it would much more difficult to reduce risk associated with the access that has been granted in the earlier stages.

1.6 Put it All Together

Requiring the subject to provide Identification, authentication and authorization as well as holding them accountable for their actions allows the integrity of the object to be maintained at a much higher level of confidence. As we have seen in the examples above, identity, authentication and authorization are required in conjunction before an object can be accessed. There are cases where a user may be able to identify themselves, authenticate but may not be authorized to perform an action beyond that. On the other hand a user may be authorized to access a resource, but is unable to identify themselves with a

proper user name. The same is true for a password credential, a user may have proper identification information but is unable to authenticate because the password the have supplied is either wrong or expired. In order for the subject to access the object each of these pieces must be present and accessible.

2 Industry Standards and Best Practices

In order to identify industry best practices and standardize access control principles there must be an entity or entities who are responsible for this role. In the case of access control standards, there are two main groups focused on these best practices.

2.1 ISO/IEC 27002

ISO/IEC 27002 is an information security standard that is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This standard specifically defines access control and how access should be managed by information security personnel. Access control is included as a section within this standard to define the best practices to suitably control logical access to network resources, applications, functions and data.

"The control objectives and controls in ISO/IEC 27002:2005 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 27002:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities." [1]

2.1 Requirements for Access Control

Key highlights of this standard include the business requirements for access control, user access management, responsibilities and definitions and best practices of the different types of access. The standard includes multiple detailed sections aimed at outlining access control for organizations so that they can implement these best practices in the most effective manner.

2.2 NIST 800-53(A)

After the Federal Information Security Management Act (FISMA) was passed in 2002 a statutory provision to ensure that agencies comply with mandatory processing standards. The National Institute of Standards (NIST) is the technology measurement and standards department was asked to develop standards and guidelines for the federal government. The NIST handbook is similar in information covered to the ISO/IEC 27002 but since it is tied to the governmental practices is goes into significantly more detail related to security controls and assessing the adequacy of the controls.

NIST 800-53 addresses multiples aspects of access, including management, technical and operational roles. [2]

3 Access Control Models

The standards and best practices from above can be used in a practical means through several different methods and models that are deemed appropriate depending on what type of security a company wants to maintain. There are many models available to use as a template for access control, but the most commonly referenced methods include least privilege, separation of duties, job rotation, mandatory access control, discretionary access control, role based access control and rule based access control. In this section we will go into greater detail about these models and their usage.

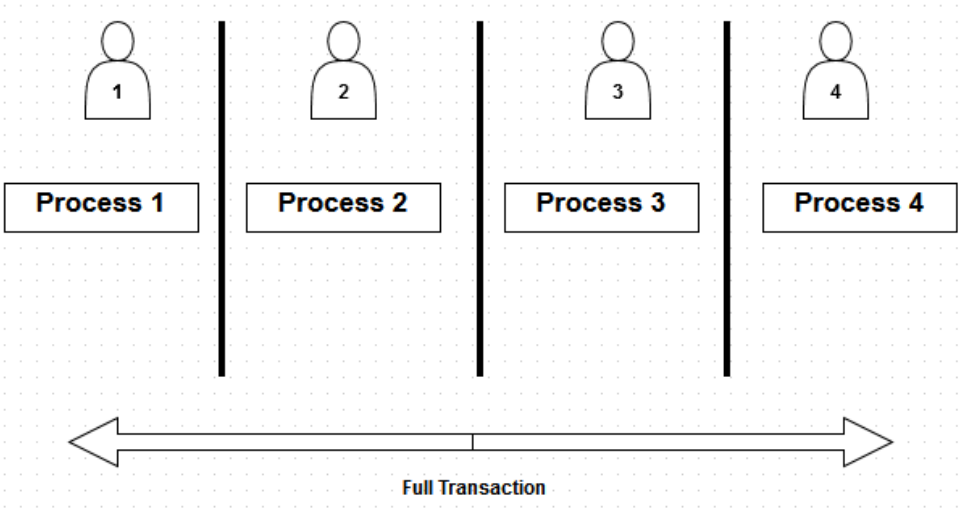
3.1 Least Privilege

The principle of least privilege is simple, no user should have any access above what is required to perform their tasks at any given time. This approach, when put into practice in its simplest form is both difficult to experience from an end user perspective and difficult to manage from an administrative perspective. In many cases users do not know what access they would need to perform their tasks and without extensive knowledge of the environment, the team provisioning the access may not know what access they need either. This method of access control does not scale well and can be prohibitively expensive and difficult to implement and maintain. Because of that, generally when this principle is used, it is used in conjunction with another approach.

3.2 Separation of Duties

The method of separation of duties states that no one person be able to handle a transaction from beginning to end. This method addresses fault or fraud by preventing someone from maliciously or accidentally initiating and completing a transaction without an additional layer of input. This method reduces the likelihood of fraud by introducing multiple variables into the process. A line of segregation is established by creating different layers of responsibility and ability to perform these transactions. This method is much like an assembly line where no single worker completely builds the finished product from start to finish. Instead each worker has their assigned task that contributes to the final product but does not create it.

Diagram 3.1 displays this method using the assembly line example to show that no one user can complete a transaction from beginning to end:



3.3 Job Rotation

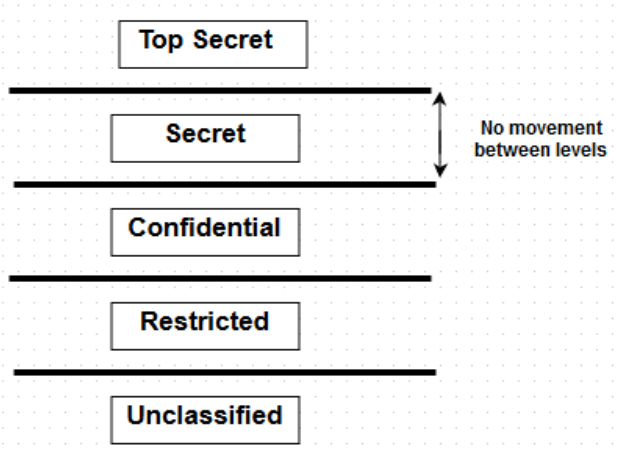
The concept of job rotation is similar to separation of duties where no one person has the ability to complete a transaction, except in this case a time limit is introduced. Job rotation requires that individuals change their roles and thus the functions they can perform at regular intervals. This rotation is to prevent exploiting a process or situation for an extended period of time. This method of access control is not typically used without the addition of another method. This method is frequently employed and has introduced several possible benefits including an increased diversity of skill and experience as well an increased job satisfaction through job change.

3.4 Mandatory Access Control

Mandatory access control or MAC is based on subject and object access level and is frequently employed in federal government and military instances. The basic principle of mandatory access control involves a central authority identifying subject's and object's appropriate access level. Subjects inherit the access to the objects at their same level. There is no access granted above their level. In some cases this method is also applied to prevent access below a subject's level as well. This method of access control is a high security and requires a great detail of management overhead because each object must be assigned a label which will then allow or deny access to subjects depending on the level assigned.

It is important to note that mandatory access control is a non-discretionary method, meaning that a user is not able to change the permissions on any object, including objects they own. Permission assignments must be performed by the central authority that is responsible for maintenance of the access control system. [3]

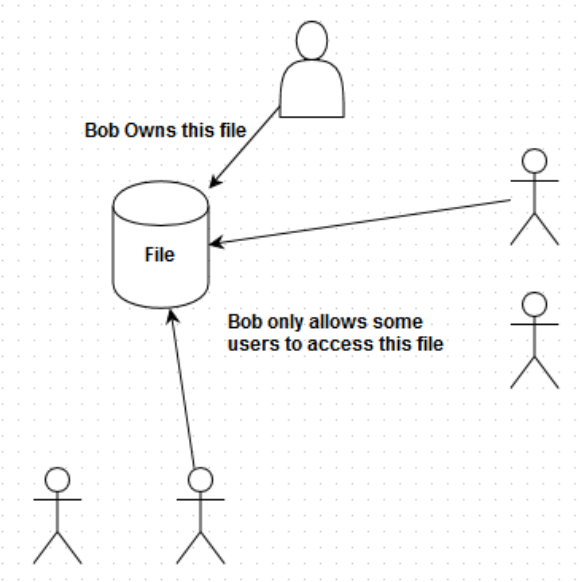
Diagram 3.2 displays the concept of mandatory access control where there is a distinct division between levels of access:



3.5 Discretionary Access Control

Discretionary access control or DAC uses the discretion of the subject to control access. DAC uses the permissions assigned by the owners of the objects to grant or deny access. This model distributes the load of access control to the subjects which removes the need for a central authority. This method is less secure than a non-discretionary access control method due to the lack of centralized authority. Decisions of access appropriateness are made by the subjects themselves and can frequently introduce risk. This method is common in small to medium sized organizations due to the reduction in overhead thus reducing cost and time necessary to implement access controls.

Diagram 3.3 displays a user granting access to an object that they own based on their own discretion:

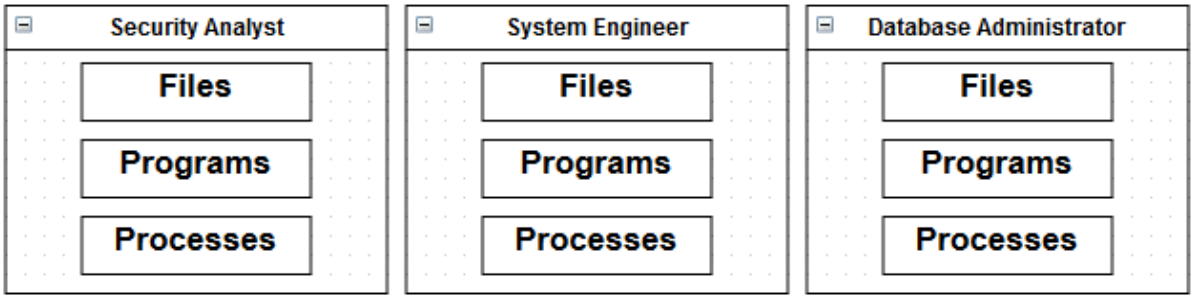


3.6 Role Based Access Control

Role based access control or RBAC requires a central authority to determine the access that will be granted to the role. Access is grouped by role across an organization and users can be in multiple groups depending on their role. No access is provided outside of access that is granted inside of the role. This practice frequently leads to providing more access than is required to complete necessary tasks. Typically, role based access control is part of a multi-level access system, like in the case of a commercial entity where there are distinct levels between necessary job roles.

Role based access control is similar to discretionary access control in that the privileges are associated with the role of the subject and not controlled by a central authority. Once a role is achieved all access is automatically granted to that user for that role.

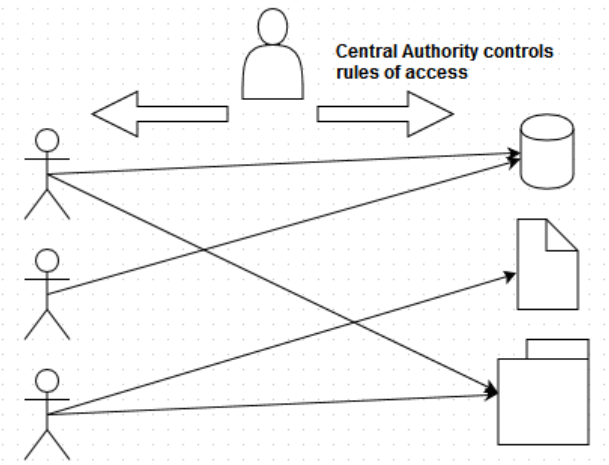
Diagram 3.4 displays how roles can be divided in an organization to allow users of the same title to access the same resources:



3.7 Rule Based Access Control

Rule based access control (also known as RBAC) uses a set of rules provisioned to subjects defined by a central authority. This method of access control is non-discretionary and can be extremely granular depending on the sensitivity of the data. Rules can be defined inside of access control lists for user access to each object. Since all permissions are controlled by a single authority, the overhead can be similar to mandatory access control. Rule based access control can also be used to permit access during a certain period of time, or could require a subject to invoke access each time they intend to use it.

Diagram 3.5 shows how a central authority can define rules for subject access to objects:



3.8 Integrated Approach

Although one method identified above can be used as an access control solution, this is not typically the case. Most organizations will choose to use a combination of these methods as they are needed based on the requirement of the organization. Using an integrated approach allows companies to base access control on their own standards and needs.

For example, a company might use role based access control for anyone with the title of database administrator, but may also use rule based access control to grant exception access beyond what is granted through the role. Additionally, a company may use a combination of rule based access control and least privilege access, where users are granted access to the objects they require only for the period of time they require them. Once access is invoked the ability to access the object only lasts for a period of time until it is automatically removed to prevent improper use.

4 Case Studies

In order to understand how these access control methods are applied it is best to relate real world scenarios that can be applied to the concepts introduced in a best practice. The following section will exemplify three cases where a combination of methods are used to create a security policy that is suited for the situation.

4.1 Case Study 1: Government/Military

In this example we will use the United States Military as the organization, but these principles can be applied broadly across governmental entities due to the relation of privilege groups. Military organizations have a defined range of classification levels that a central authority is responsible for assigning. This non-discretionary access method is the most demanding, but is necessary given the sensitivity of the data. These classifications include top secret, secret, confidential, restricted and unclassified. Starting at the bottom, unclassified data has been made available to the public, and top secret data is only available to the subjects who have the proper clearance, or access.

This military access control method follows the mandatory access control model, which prevents subjects and objects from reading above and in some cases writing below the access level granted. An engineer with a confidential level clearance is not able to read data above the confidential classification and a subject with a restricted level clearance is not able to write data that is unclassified.

The objective of this mandatory access control is to first identify what type of data or object you have and then allow subjects with that equal access to use it. This type of access control requires a central authority to make the decisions about the classification of the subjects as well as classification of the objects. There is no discretion given to the subjects because they may not make the right decision about the access level, even with data they create.

This type of access control method is extremely time consuming, expensive and has a high level of overhead to maintain, but it is necessary in order to keep the most sensitive data secure from individuals who should not have access to it.

4.2 Case Study 2: Large Financial Company

In this example, we introduce a large financial company with extremely sensitive personal customer data to protect. This company does not have the same security levels defined as the military organization from the example above. Instead of the use of mandatory access control, the financial company will use an integrated approach combining methods based on the type of access and the user that will access it. The most common approach will be based on the role of the subject. Multiple rules will be defined for a single role, and a user is only allowed to be in one role at a time. On top of this access, subjects will be granted exception or rule based access to objects that are required beyond their role. This type of access is necessary to prevent subjects from gaining unnecessary access from a role and maintains this exception access through a central authority.

In order to be added to a role and then given rule exception access subjects must be granted this approval by the custodians or owners of the role and applications inside of rules. This prevents users from granting access to themselves and provides an audit trail that access was approved based on a defined business justification for each user.

The most privileged access in this large financial company is write access on a trading platform, so this access is managed through a special type of rule based access control that uses the concept of least privilege. Users must invoke their access to these functions only when they need them. Once the access is invoked, the functions are available to them, but they have a limited of time (usually less than 24 hours) to perform their required actions before the access is lost.

Financial companies have a wide range of subjects and objects which is why a centrally managed administration authority is essential to enforcing the policy and mitigating risk to the firm. Users in this instance also play a key role because they are the most knowledgeable about what they need to perform their duties, and any access above this function must be removed.

4.3 Case Study 3: Small Internet Sales Company

The final case study involves less sensitive data and is a typical scenario for most small businesses like an internet sales company. For this example the company has a sales and marketing department, human resources, and a technology department. Each department has data that should not be available to the other groups, but the company lacks the time and money required to centralize the authority of access to this data.

Discretionary access allows the subjects to assign the privileges to the objects they own and maintain. A human resources analyst who holds the salary information of all employees will make this document only available to those in her department because of the sensitivity of the data. This is done using a Windows access control rule that allows only a certain number of employees to access this data.

Similarly the sales manager who has access to company sales statistics and records does not share this data with anyone but those who are authorized to see it. In some cases, data can move between groups especially in the example of a technology engineer who owns a database that houses the employee directory. This data is accessible to everyone because it is something everyone needs.

DAC has very low overhead in this situation and the responsibility is on the subjects to maintain access control. The risk is higher in this type of example for that reason, but small companies take this type of risk because is necessary to avoid the cost of another more involved solution.

5 Closing

Managing access control can be approached in different ways. But in the end, in order for the system to function effectively at its most basic level, a subject must have access to an object in order to perform its required task. Controlling this access based on a predefined rule is essential to mitigate risk of the object being unprotected.

In order to achieve this function, the subject must first properly identify itself, adequately authenticate to the system and then be appropriately authorized to perform the action it is requesting. In most cases this is done though an integrated process created based on the need of the entity responsible for the objects. Without the methods, there would be no reason to control access because there would be no system at all.

6 References

[1] Disterer. (2013). Iso/iec 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(92-100)

[2] Locke. (2009). Recommended security controls for federal information systems and organizations. *3*(800-53)

[3] Osborn. (n.d.). Mandatory access control and role-based access control revisited. 31-40.

Ballad, B. (2010). *Access control, authentication, and public key infrastructure*. (pp. 238-264). Sudbury, MA: Jones & Bartlett Learning.

Cascarino, R. (2012). *Auditor's guide to it auditing, second edition*. Hoboken, NJ: John Wiley & Sons Inc.

Dubrawsky, I. (2009). *Eleventh hour security*. (pp. 92-101). Burlington, MA: Elsevier Inc.

Ferraiolo, D., Cugini, J., & Kuhn, R. (n.d.). Retrieved from http://csrc.nist.gov/groups/SNS/rbac/documents/ferraiolo-cugini-kuhn-95.pdf

NIST. (n.d.). Retrieved from website: http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf

Seidl, D. (2013). *Comptia security training kit*. (pp. 380-386). Sebastopo, CAl: O'Reilly Media, Inc.

Techotopia.com. (n.d.). Retrieved from http://www.techotopia.com/index.php/Mandatory,_Discretionary,_Role_and_Rule_Based_Access_Control