Global Information Assurance Certification Paper

Rhonda M. Furst
GSEC Practical Assignment
Option 1
April 14, 2004
Version 1.4b

Role Based Access Controls (RBAC): Balancing an Organization's Business and Security Needs

Abstract

Organizations continuously push for shortened time to market, as they strive to be the first to implement a new technology in their quest to develop a better way of doing business. While rushing to implement a new product, access to security information and systems can become a nightmare for developers and business areas. Working with security professionals and access administrators to determine what access is needed can be time consuming and very frustrating for those whose main focus is to produce a product in the shortest time possible or who need to expediently carry out the business of the day. While security has always been viewed as a necessary evil, in the mad rush to produce a newer/better product, security can be considered the stop sign of progress. Role based access controls can eliminate the stop sign posted at each individual access request by researching, grouping, and getting pre-approval for all access for a specific role before it is needed.

The RBAC software available to run a role based access control process adds technology to the role based access control process. However, my paper will focus on the process of defining structures and roles to be entered into a chosen application. The paper will illustrate how security policies can be strengthened by creation of access based on roles versus individuals, and how at the same time access to information and systems can be a quicker and easier process, creating a balance between an organization's business and security of its information and systems.

Why Role Based Access Controls?

Security is intended to be a stop sign. Running parallel with the push to shorten time to market is the ever increasing need to secure an organization's information and systems by allowing only the access needed to perform one's job function. In other words, security raises the stop sign long enough to perform a check of an individual's credentials by asking, "Does Bob really need the information he is trying to access?"

Role based access control systems enable organizations to better secure information and systems while considering the needs of business areas and developers. Administration of security access to information and systems, especially in large organizations, is an arduous task. Working with business partners to determine what an individual needs to do their job requires knowledge of security policy, as well as knowledge of the business. Business, as defined in the American Heritage College Dictionary is "the occupation, work, or trade in which a person is engaged." In other words, business is the job or role an individual performs in their employment. If an organization is large, it is virtually impossible for security professionals/administrators to know the access needed for every job function in every department.

"The traditional approach to controlling access to information and network resources is to establish specific permissions for each user. While effective in a static environment, the approach is often difficult to manage in dynamic environments where users enter and leave or change positions within the organization" (Kropp). The larger the organization, the more roles and people change, which complicates administration of access. Information and systems used by an individual a few years ago may not be the same ones used today. The need for increased flexibility has lead larger organizations to explore role-based access controls. Specific permissions are grouped depending on the individual's job function or role.

"Role-based access control is a relatively new approach that maps to organizational-specific structures, improving security and reducing administrative cost by granting users access to applications, information and networks based on their role and not their individual identity" (Kropp). With role based access controls, the days of comparing one employee to another or struggling to determine what access is needed on an individual basis are over, and instead access is determined by the role or job function of the individual. Access can be grouped within roles that allow an area to request access to all information and systems with the submission of one pre-approved request. When an employee leaves the role, all accesses are deleted in the same manner, eliminating the risk of unneeded access following an individual throughout their career within the organization.

In a role based access control system, roles grant access to information and systems needed by individuals to perform duties associated with the job they perform. With research and advanced approval from data owners, an organization achieves a balance between security and business need by allowing easy access after detailed research. "Security is a question of balance. Too little security leaves your company vulnerable, but an overemphasis on security gets in the way of attending to business, inhibiting the company's growth and prosperity. The challenge is to achieve a balance between security and productivity" (Mitnick, 10). Security is a business, and role based access controls allow a win/win for both security professionals and business areas.

Further Defining Role Based Access Controls

"Access is the ability to do something with a computer resource (e.g., use, change, or view). Access control is the means by which the ability is explicitly enabled or restricted in some way (usually through physical and system-based controls)" (NIST/ITL Bulletin). Role based access controls enable access by creation of roles associated with the duties an individual performs.

To further define, "when a user is associated with a role: the user can be given no more privilege than is necessary to perform the job. This concept is least

privilege and allows the user no more or less access than required. The concept of least privilege requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more" (NIST/ITL Bulletin). Maintaining strict access controls with traditional administration is complex, as job roles change and the access needed within the role tends to overlap into other roles making a clear definition difficult. Security professionals must continuously review and revise established security policies to determine what access is adequate and what access exceeds that which is needed. Many times more access is granted than needed, or not enough access is granted and business areas must resubmit requests numerous times.

To show the advantages of role based access controls, I'll illustrate a scenario utilizing traditional security access administration. As stated, many security access administration areas grant access privileges to information and systems based on an individual's need. Sally states, "I'm a new Accounting Specialist in payroll and need access to salary and tax information. An individual who maintains a list of the groups needed to get this access submits forms to obtain the appropriate groups. For practical purposes we'll refer to these groups as S and T. Approved request forms are forwarded to an access administration area and the Accounting Specialist is granted access to the requested groups.

However, during the course of doing business, Sally discovers her co-worker, Tina has access to a new application that allows her to verify salary and tax information with the click of a button. Tina doesn't know what group allowed her access to the application, and instructs Sally to call access administration for assistance. Sally asks access administration to help her determine what groups grant access to the click application.

To determine what Sally needs, an administrator will ask for the specific group name. Since Sally doesn't know the specific group name, the administrator may be asked to look up Tina's id, and do a comparison. Since it is difficult for an administrator, not knowing the business, to determine what access is associated with the existing group, the administrator informs Sally that Tina has access to groups C and D, as well as S and T, and her area should determine which one is necessary to gain access to the click application. Unable to determine which group grants access to the application, Sally completes an access request for groups C and D, believing these groups will give her access to the click application, and receives approval from the authorizer. While access to C and D grant access to the application, neither Sally nor the administrator realize that along with the click application, access to group D has given her access to employee financial institution account numbers associated with Tina's previous duty as Draft Specialist in the same department.

How did this happen? Tina moved on from her Draft Specialist responsibilities to Accounting Specialist. Individuals responsible for requesting access for the new

role requested the new access and failed to remove the old access. By granting individual access, Sally has the unneeded access, as well. In short, the process of granting access per individual allowed for human error that opened a security risk for the company and does not adhere to the least privilege security policy. Sally has more access than is needed for her role, and incorrect access was approved by an authorized individual. (NIST/ITL Bulletin)

While the above illustrates just one scenario, it does identify several concerns associated with traditional access.

1. Excessive individual access. Unless Sally realizes and reports the unneeded access, she will retain access to confidential information.

2. Delay receiving needed access. Sally's area submitted a form for access they believed would allow her to do her job. After Sally discovered she needed the additional access to do her job more efficiently, she had to contact the access administration area to determine what access was needed and submit another form to receive the additional access. Unless Sally reports the additional access received to the individual submitting the initial form, every new Accounting Specialist will experience a delay receiving access needed to effectively perform their role.

3. Opening a security risk. By comparing Sally's access to Tina's, too much access was granted. Too much access creates an information security risk. In this case, Sally has access to financial institution account numbers for all employees in the organization.

4. Deletion of unneeded access. With traditional access administration, there is no reliable method of deleting unneeded access. The result – An individual carries old access privileges from job to job through his/her career.

"With role-based access controls, access decisions are based on the roles individual users have as part of an organization. Users take on assigned roles (such as doctor, nurse, teller, manager). The process of defining roles should be based on a thorough analysis of how an organization operates and should include input from a wide spectrum of users in an organization" (NIST/ITL Bulletin). Role based access restricts access to that needed for a specific role and grants access based on the role. Role-based access removes the guesswork of access administration, and predefines what is needed, increasing security of an organization's information and systems.

If role based access controls were in place in the above referenced organization, Accounting and Draft Specialist roles would exist. When Tina moved from Draft Specialist responsibilities to Accounting Specialist, the Draft Specialist role would

be deleted and the Accounting Specialist added. With upfront research, all needed accesses would be grouped and updated on a regular basis to include any new information, applications, systems, etc. Information systems would be maintained with accurate security access to adhere to the organization's security policy and auditing regulations.

Benefits of Role Based Access Control Systems

"Various surveys have found that a significant number of organizations have experienced an insider security lapse, costing an average of about a quarter-million dollars per incident" (Kropp). While those in the security field see access control as necessary to keeping a company's information systems secure, business areas see security as an unnecessary and annoying delay that works against getting the job done. A manager who hears the employee complaints, who are sitting idle because they cannot get access to do their jobs, sees a lapse in productivity – Dollars spent with nothing in return. Business areas are frustrated with the perceived unnecessary red tape required when requesting security access, and become impatient with their inability to do business. This in turn frustrates security professionals/administrators as they strive to protect the company's information and systems assets while maintaining customer service. All this many times leads to holes in security brought about by a frustration and directives to give the individual what is needed. And frustration sometimes leads to a security breach that puts the organization's security policy enforcement in jeopardy.

Another business area frustration is the need to submit numerous access request forms. A business area must understand on what system the information or application resides, which results in the submission of numerous forms, and knowledge of how to complete those forms, along with how to request the correct access to allow the employee to do their job. Access overlaps roles, which adds complexity to the access granting process, and sometimes requires verification from numerous approvers/areas. And of most concern, there may be times when too much access is unknowingly granted a business partner trying to gain access to information and systems needed to perform their job.

Role based access control systems increase internal security by maintaining tighter control of individual access, allowing users to request access privileges by role (Kropp). The same access is granted every time to every individual who performs the role through a profile associated with that role. If access within the role changes the profile is modified to add or remove the access. If an individual moves on to another role, access can be easily deleted and new access granted via profiles created by role based access controls administrators. To illustrate the role based access control model, I've included the following diagram.

Traditional Access Admin	Users ====> Access Privilege
Role Based Access Control	Users ====> Role ====== > Access Privilege

"Role-based access controls can implement sophisticated security policies that are difficult to implement otherwise. This of course is impossible in systems where there is a pre-defined and immutable superuser, and anyone occasionally needing access to more privileges than granted to ordinary users must necessarily be granted the highest level of privileges" (Cygnacom). Policies will be consistently enforced through predefined roles with users requesting access for a specific timeframe for all accesses needed, rather than individually through numerous access request forms to specific security platforms. Utilizing role based access controls will ensure all users have the access needed to do their job, no more and no less.

"Separation of duties can be either automatically enforced or procedurally supported depending on the implementation" (Cygnacom). Access can be granted through roles containing programmatic groups allowing for automated access or manually by coordinators in the business area who can determine if access is needed and if it is, for what duration.

Role based access administration is concerned with the coordination of accesses into roles and maintenance of those roles. Once necessary access is defined within the role and has been created, administration of access is relatively simple. The system dictates what access should be granted, and whether access is granted manually or through automation (a purchased RBAC system), administration is provided in a more timely and accurate manner. The table below is an estimate of administration time savings realized.

TABLE 1: **ESTIMATED TIME (IN MINUTES) REQUIRED FOR ACCESS ADMINISTRATIVE TASKS**

TASK	RBAC	NON-RBAC	DIFFERENCE
Assign existing privileges to new users	6.14	11.39	5.25
Change existing users' privileges	9.29	10.24	0.95
Establish new privileges for existing users	8.86	9.26	0.40
Termination of privileges	0.81	1.32	0.51

(Kropp)

Role based access controls save time for administrators and users, which translates to money, while providing tighter, more controlled security for the organization.

How Do Role Based Access Controls Work?

Although discussion of the numerous RBAC applications that can be purchased to maintain role based access controls and how they work is important, it is the

preliminary research and defining of roles that is crucial to the system's success. As with any security application it is the process/policy put in place that allows the application to function at its highest level, and allows security professionals to enforce any security breaches that may occur. Therefore, careful preparation and research, structuring, and role definition is needed before a role based access control system can be implemented.

Most Security policy is written to invoke the least privilege model. "The principle of least privilege requires that a user be given no more privilege than necessary to perform a job. Ensuring least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to a domain with those privileges and nothing more" (Ferraiolo). Least privilege demands security administrators/professionals and business areas look at a job function or role and determine the least access required to effectively perform the role. To ensure roles are defined by least privilege, the following will be considered.

- Roles are assigned based on organizational structure with emphasis on the organizational security policy
- Roles are assigned by the administrator based on relative relationships within the organization or user base. For instance, a manager would have certain authorized transactions over his employees. An administrator would have certain authorized transactions over his specific realm of duties (backup, account creation, etc.)
- Each role is designated a profile that includes all authorized commands, transactions, and allowable information access.
- Roles are granted permissions based on the principle of least privilege.
- Roles are determined with a separation of duties in mind so that a developer Role should not overlap a QA tester Role.
- Roles are activated statically and dynamically as appropriate to certain relational triggers (help desk queue, security alert, initiation of a new project, etc.)
- Roles can be only be transferred or delegated using strict sign-offs and procedures.
- Roles are managed centrally by a security administrator or project leader. (CGI Security)

You will also need to consider the possible activities associated with defining and modifying roles:

- Add a role and its associated information/applications.

- Delete a role and its associated information/applications.
- Modify an existing role:
    - Add
    - Remove
    - Modify (Barkley)

As you can see from the extensive list of considerations, defining roles is a time-consuming task. It is best to work with a contact from a business area to gather a list of privileges required to access information and systems used by their area.

Once the information is gathered, you will need to determine who owns the information/system and get their approval to add it to the role. You will find the task to be somewhat frustrating, as original data owners may have moved on to another responsibility or left the organization, but time spent diligently determining data owner(s) will ensure the integrity of your role based access control system.

Once you've received a data owner's approval, you will need to file the approval for future reference and review and add the approved access to the role. You'll need to follow the established role defining procedure for each piece of information/system access associated with the role.

You will also need to work with the business areas to assign coordinators who will be submitting access requests through the role based access control system. The individuals should be directly associated with and have knowledge of the specific roles within the business. It is essential there be at least two coordinators associated with each role for business continuity purposes.

Again, it is important to remember a critical aspect of the role based access control system is accurate and thoroughly researched roles. That is why it is important to work with the business area to:

- **Define role based access control requirements**. Initial determination of roles and structure of those roles is imperative to an accurate access grouping.
- **Define roles** – Positions and jobs performed in the business area must be defined. Again, the more specific the role, the more accurate the access.
- **Determine access** – What access is needed to perform the job.
- **Locate information/system owners**. Thoroughly research who owns specific data. The business area should be able to assist in this process.
- **Receive approval from information/system owners**. When granting approval, owners must realize they are granting approval for all individuals in a specific role.

- **Create Profiles and assigned Profile owners**. Profiles are created for the defined roles with a minimum of two Profile owners assigned. Security policy should define the required organizational level of the Profile owners (management, analyst, etc.).
- **Accurately input information in the role based access control system**. Information should be checked for accuracy before implementation.
- **Communicate**. Communication is key to successful implementation. Role based access controls administrators and business area contacts must remain in constant communication throughout the process. It is key that an accurate and complete profile is created enabling users to receive all access via the initial request.
- **Schedule and perform periodic review of profile(s)**. Profiles must be reviewed periodically to ensure they contain up-to-date information. A policy should be put in place to define creation and maintenance of roles, with specific timelines for review. The role based access controls administrator and business area should review the profile within a set timeframe to ensure it continues to be valid and up-to-date. (CGI Security)

Stepping Through the Role Based Access Control Process

Let's create two Profiles. We'll go back to the Accounting Department and define two existing roles – Accounting Specialist and Draft Specialist.

Step 1: First you must decide how your role based access controls system will be structured. Will you structure it to include every role, or can some roles be combined. Will you start from the top down, management to administrative, most sensitive data to least or will you build least to most. Determining structure can start with a review of the organization's business structure, current security policy to determine how access is granted and the philosophy of that security policy. In most, if not all cases, security policy is written to defend least privilege, and with a role based access control system you are one step closer to ensuring your policy is easily enforceable.

- Security professionals and the role based access controls administrators met to discuss how to structure the system, and it was decided profiles would be created from job functions building on the least privilege model, access is added on, as needed.

Step 2: Once structure is determined and policy is in place to define your role based access system, you'll need to contact a business area. It would be best to begin with a pilot area when creating the first Profiles. Once an area is identified you'll need to ask for one or two contacts to assist with defining roles and determining security access needed. You'll need to meet with your business contact(s) to determine what their area does and what kind of access is needed and have them submit a list of roles and associated accesses.

- The role based access control administrator met with Accounting, and Sally was assigned as the business area contact. Sally explained the roles within the department. Sally wanted to start with the Accounting and Draft Specialist roles. The role based access control administrator asked her to compile a list of all necessary accesses and authorizer.

- The list was forwarded to the administration area with group name and authorizer(s) for review.

Accounting Specialist	**Draft Specialist**
Group S -- Management	Group S -- Management
Group T -- Management	Group T -- Management
Group C -- Management	Group C -- Management
Group D -- Management	Group D -- Management

Step 3: After the contact has submitted a list with roles and associated accesses, you'll want to group the role's access into a profile and go over requirements with your business area contact. This is where you'll work closely with the contact to identify data owners and seek their approval. You'll also need to work with the contact to determine who will own the Profiles. As work schedules sometimes delay this part of the process, you'll need to be in constant communication with your business contact to ensure the process proceeds in a timely manner and all information is gathered for entry into the system.

- In this case, profiles will be named Accounting Specialist and Draft Specialist under the Accounting Department umbrella.
- The administration area worked with Sally to determine who owned the data.
- Sally and the Accounting Manager will own the Profiles for maintenance (add, delete, change) purposes. Sally will be responsible for all modifications and the Accounting Manager will have the authority to enforce those changes.

Step 4: Once data owner approval has been obtained, the next step is to accurately input information into your role based access controls system. Profiles should take on the role name for easy identification by the business area coordinator. Accuracy is imperative to successful creation of a profile. While profiles can be modified, as needed, it is important they are accurate at implementation. There is nothing that undermines the confidence of your business areas more than producing a product that needs immediate updates and corrections or worse, provides incorrect access.

- During research, it was determined Group D's data owner was different from the others. Sally and the administrator contacted Group D's owner and discovered the group gave access to the associate financial institution

account numbers. Since Sally, the Accounting Specialist, could determine access was not needed for her role, she returned to consult the Draft area to determine if it was needed for the Draft Specialist role.
- The access was needed for the Draft Specialist, as that role is responsible for ensuring an associate's pay is deposited into the correct account.
- Data owners granted approval for access to their data to the Accounting and Draft Specialist roles.
- Profiles were regrouped to show correct access and data owner.

Step 5: The last step is to send a completed copy of all Profiles and associated access to your contact for final review. Once approved, determine specified timelines for periodic review agreed upon with your business area contact(s), and you are ready for implementation.

- The final profiles were grouped with the correct access and data owners

Accounting Specialist		**Draft Specialist**	
Group	**Data Owner**	**Group**	**Data Owner**
Group S	Bill Smith	Group S	Bill Smith
Group T	Bill Smith	Group T	Bill Smith
Group C	Bill Smith	Group C	Bill Smith
		Group D	Dave Jones

- It was determined a yearly review of existing roles would be sufficient. The date was entered on the team calendar by the Role Based Access Controls Administration area.
- Profiles were entered into the RBAC system, and implemented after final review.

Although the example illustrated is simplistic, you can see the process can be slow, tedious, and requires constant follow up, but the end result will be time and cost savings, as well as increased security for your organization. In this case, after research it was determined Group D, that was approved by management, was being granted to associates who did not need the access to perform their job. With good communication and follow up with the business areas by Role Based Access Control Administrators, the correct roles can be defined and kept up-to-date, enabling the role based access control system to provide accurate security access to business partners.

Role Based Access Controls – A Perfect System?

Does the role based access control system sound too good to be true? Role based access control systems appear to be perfect. How could a hole develop in the security infrastructure when access is administered by roles that are specifically defined to ensure least privilege? With careful research and coordination, roles are defined to grant appropriate access. However, there is

one problem not addressed by role based access, “limiting a client to only one specific account means that authorization is based not only on a specific method, but also on specific parameters to that method” (Sessions 90). Controlling the access an individual is granted does not verify the individual is really who he says he is, but rather that an account exists that has been identified within a specific job function. If roles or positions are not clearly defined in the company’s directory, it will be difficult to determine if an individual who states he/she is performing a specific role, really is performing that role.

However, if your role based access control system assigns knowledgeable business area coordinators to police roles, those coordinators should research to verify an individual is in a specific area performing a specific role, before a role based access controls request is submitted for processing. While role based access control removes the human element from access administration, verification of those requesting access through the system rests with the business area to verify the individuals are who they say they are.

Conclusion

Role based security access controls eliminate administration guesswork and time spent by administrators determining access needed from individual request forms. Accurate access administration will be achieved by either automation of accesses or clearer and more explicit instructions to an administrator regarding accesses allowed under the profile. The result, less returned forms to business areas asking for additional information, increased user satisfaction due to a less complex way of requesting access, and controlled security accesses put in place by policies and procedures that will protect against unauthorized access.

Role based access control systems add convenience to business areas while maintaining information systems integrity. The coordination of role based access controls enables secure systems where individuals receive what they need, and no more. As stated, the role based access control system is a relatively new concept and requires research and attention to detail while creating roles. However, the end result will be increased productivity and cost savings, as companies become experienced in defining roles and the stress of submitting use forms by business areas becomes a thing of the past.

Role based access control systems provide a more secure environment, while enabling customer service to business areas, creating balance between business and security. Granting access through a role based access administration system is a more efficient way to provide access to individuals in a time when producing results or time to market is the difference between a company’s failure and success.

Works Cited

American Heritage College Dictionary. Boston: Houghton Mifflin Company, 1997.

Barkley, John. First ACM Workshop on Role Based Access Control. 4-14-2004 http://hissa.ncsl.nist.gov/rbac/rbacot/titlewkshp.html.

CGI Security. A Guide to Building Secure Web Applications. The Open Web Application Security Project (OWASP). 4-14-2004 http://www.cgisecurity.com/owasp/html/ch08s03.html.

Cygnacom. NIST Role Based Access Control. 4-14-2004 http://www.cygnacom.com/labsOLD/backup/act022.htm.

Ferraiolo, David and Kuhn, Richard. Role-based access controls. Proceedings of the 15th National Computer Security Conference, Vol II, pp 554-563. 4-14-2004 http://hissa.ncsl.nist.gov/rbac/paper/rbac1.html.

Kropp, Brian and Gallagher, Michael. Access to Cost Savings. Role-based access control systems can save organizations time and money. Information Security Magazine. 4-14-2004 http://infosecuritymag.techtarget.com/articles/april01/cover.shtml.

Mitnick, Kevin. The Art of Deception. New York: Wiley Publishing, Inc. 2002.

NIST/ITL Bulletin. An Introduction to Role Based Access Control. 4-14-2004 http://csrc.nist.gov/rbac/NIST-ITL-RBAC-bulletin.html.

Sessions, Roger. Software Fortresses, Modeling Enterprise Architectures. New York: Addison Wesley, February 2003.