Concordia University College of Alberta

Master of Information Systems Security Management (MISSM) Program

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

AN EVALUATION OF A GOVERNMENT ORGANIZATION'S INFORMATION SYSTEMS ACCESS CONTROL PROCESS:

ISSUES AND PROPOSED SOLUTIONS BASED ON ROLE-BASED ACCESS CONTROL METHODOLOGY

by

MA, Billy

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

Date: May 2009

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Dale Lindskog, Associate Professor, MISSM

AN EVALUATION OF A GOVERNMENT ORGANIZATION'S INFORMATION SYSTEMS ACCESS CONTROL PROCESS:

ISSUES AND PROPOSED SOLUTIONS BASED ON ROLE-BASED ACCESS CONTROL METHODOLOGY

by

MA, Billy

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Dale Lindskog, Associate Professor, MISSM

Reviews Committee:

Andy Igonor, Assistant Professor, MISSM
Dale Lindskog, Assistant Professor, MISSM
Ron Ruhl, Assistant Professor, MISSM
Pavol Zavarsky, Associate Professor, MISSM

The author acknowledges the significant contributions to the work by Academic Advisors and Review Committee Members and gives the right to Concordia Univeristy College to reproduce the work for the Concordia Library, Concordia Websites and Concordia MISSM classes.

AN EVALUATION OF A GOVERNMENT ORGANIZATION'S INFORMATION SYSTEMS ACCESS CONTROL PROCESS:

ISSUES AND PROPOSED SOLUTIONS BASED ON ROLE-BASED ACCESS CONTROL METHODOLOGY

by

Billy Ma

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

Concordia University College of Alberta

Date: July 29, 2008

Research Advisor:
Dale Lindskog
Assistant Professor, Information Systems Security Management Program
Concordia University College of Alberta

Subject Matter Advisor:
J. C. Mercier
Manager of Information Security
Government of Alberta

Concordia University College of Alberta

Abstract

AN EVALUATION OF A GOVERNMENT ORGANIZATION'S INFORMATION SYSTEMS ACCESS CONTROL PROCESS:

ISSUES AND PROPOSED SOLUTIONS BASED ON ROLE-BASED ACCESS CONTROL METHODOLOGY

By Billy Ma

This research paper will review and evaluate a bona fide government organization's information systems security access control and audit process. From this review, the research paper will identify three major areas of concern with the existing access control process. The first is *Systems Administration*, the second is *Systems Security*, and finally is the *Systems Auditing Process*. After these issues have been identified, this research paper will propose to utilize Role-Based Access Control Methodology as a solution to address each of these issues.

TABLE OF CONTENTS

LIST OF FIGURES

Number

1 Introduction

Computer systems have become a part of our daily lives—both at home and at work. At home, accessing our personal computer is as simple as turning on our computer. However, in the workplace it becomes more complicated. As users within an organization, we all have to go through an identification, authentication, and authorization process to access information on a computer. In today's highly technical business world, organizations have become enormously dependent on computer systems and software to drive their businesses. As a result, there are now numerous application systems and resources that are accessed daily by users to fulfill their functions. With the growing number of users accessing these resources, the logistics of maintaining control and security over the use of these resources is nearly impossible without some sort of access control methodology. Therefore, it is imperative that "organizations develop and enforce access policies that protect sensitive and confidential information; prevent conflict of interest; and protect these systems and its content from intentional and unintentional damage, theft, and unauthorized disclosure" (RIT, 2002).

Organizations are facing important and unprecedented challenges in an ever dynamic, constantly changing, and highly complex computer environment (eg. see Ferraiolo, 2007 & RIT, 2002). As more changes occur in an organization, the more complex and time consuming it is to administratively maintain control, enforce security and audit these systems. For this reason, this research paper will look at a bona fide government organization and describe and evaluate its existing information systems access control and auditing process in detail. While this organization has used this process for a period of time, the Researcher will demonstrate that there are three areas that can be improved upon. These

three areas of concerns are (1) *Systems Administration,* (2) *Systems Security* and (3) *the Systems Auditing Process.* This paper will detail all three areas of concern and will propose to utilize Role-Based Access Control Methodology (RBAC) as a solution to address each of these issues.

2 The Government Organization

This research paper will take an in-depth look at a bona fide, regulated government organization (which will be referred to as the Organization) and review how the access of information is managed. Before we can describe how this Organization manages its information systems access, we must first take a look at the Organization's structure and systems. This Organization consists of approximately 830 employees throughout the province that require access to a number of large servers and an even greater number of applications—both in-house developed applications and commercial applications. Here are two important aspects of the Organization that we must first look at and understand before we can detail how the Organization manages it access control.

First, is the Organizational Structure:

- Consists of a Governing Board – One Chairman and Six Board Members
- Chief Executive Officer
- Eight (8) Divisions
- Twenty-three (23) Branches
- One Central Office and Four Area Offices Throughout the Province
- Over 830 Employees

Second, is the Information Systems Structure:

- Applications

- 35 In-House Developed (based on existing OS)
- 3 Commercial

➢ Domain Statistics

- Number of UserID's: 1056
- Number of Special Id's: 231
- Number of Security Groups: 527

➢ File System Statistics

- Number of Top Level Folders: 59
- Number of 2nd Level Folders: 828
- Total Number of Folders and Sub-folders: 75000+

2.1 Information Systems Access Control Process:

This section will describe the administrative process of how permissions are granted to users within the Organization. This will be broken down into two parts. This first is how new users are granted access permissions and the second is how changes are made to access permissions for existing users transferring to new positions.

For a new user, this process begins after having gone through the Human Resources selection process. Once an individual is hired, Human Resources will notify the Manager of the new employee. The Manager then completes a Systems Access Request (SAR) form (see Figure 1). This form is essentially a checklist, which consists of applications and databases (resources) that are part of the Organization's information systems.

Figure 1. System Access Request Form

SYSTEM ACCESS REQUEST

REQUESTS FOR NEW NETWORK USERID'S, COMPUTER EQUIPMENT OR PHONES REQUIRE ONE WEEK'S NOTICE

Client Name: _____ Extension: _____ Client Status: ☐ New Employee ☐ Transferring

Division/Section: _____ Location/Floor: _____

Client Access Similar to: _____
if possible, please print name of person who has similar access to requested individual

Manager's Approval: _____ Required by: _____
please print name and initial date

	Installed by		Installed by
☐ Action Request System		☐ Licensing Registration	
☐ AS400		☐ Licensing ***	
☐ BackOffice		☐ LMS (Licensing Management System)	
☐ ******Link		☐ LTC Reporting	
☐ *******Track		☐ Outlook	
☐ CFEP		☐ Outlook Web Access (please attach justification)	
☐ Citrix/RSA Token (attach justification)		☐ Pager	
☐ Clientele Help Desk		☐ Payroll / HR	
☐ Clientele Hotline		☐ PC and/or Laptop	
☐ CORES		☐ PRISM (WCLC form required)	
☐ Customs & Excise		☐ Pro Com Plus	
☐ EZPay		☐ Product & Pricing	
☐ FGRS		☐ PROSYS	
☐ Fleet Management		☐ RIBS	
☐ Forest & Trees		☐ RICE	
☐ GLS		☐ Telephone (16 button)	
☐ GMIS		☐ Telephone (8 button)	
☐ IRSS		☐ Telephone Headset	
☐ IVR Banking		☐ Versatile	
☐ JDE		☐ VIPER	
☐ LAN Standard Menus / Icons		☐ Visio	
☐ Last Name Change		☐ Voice Mail Box	
☐ LDIS		☐ Other _____	
☐ LFIS		☐ Other _____	

Please provide optional additional information below, if required. **Include the equipment tag # if applicable**:

INFORMATION SYSTEMS USE ONLY

SECURITY GROUPS

AS400 / JDE Access

Same As: _____
User ID: _____
Temp Password: _____
Completion Date: _____
Client Notification Date: _____

Windows 2000

User ID: _____
Temp Password: _____
Initials: _____

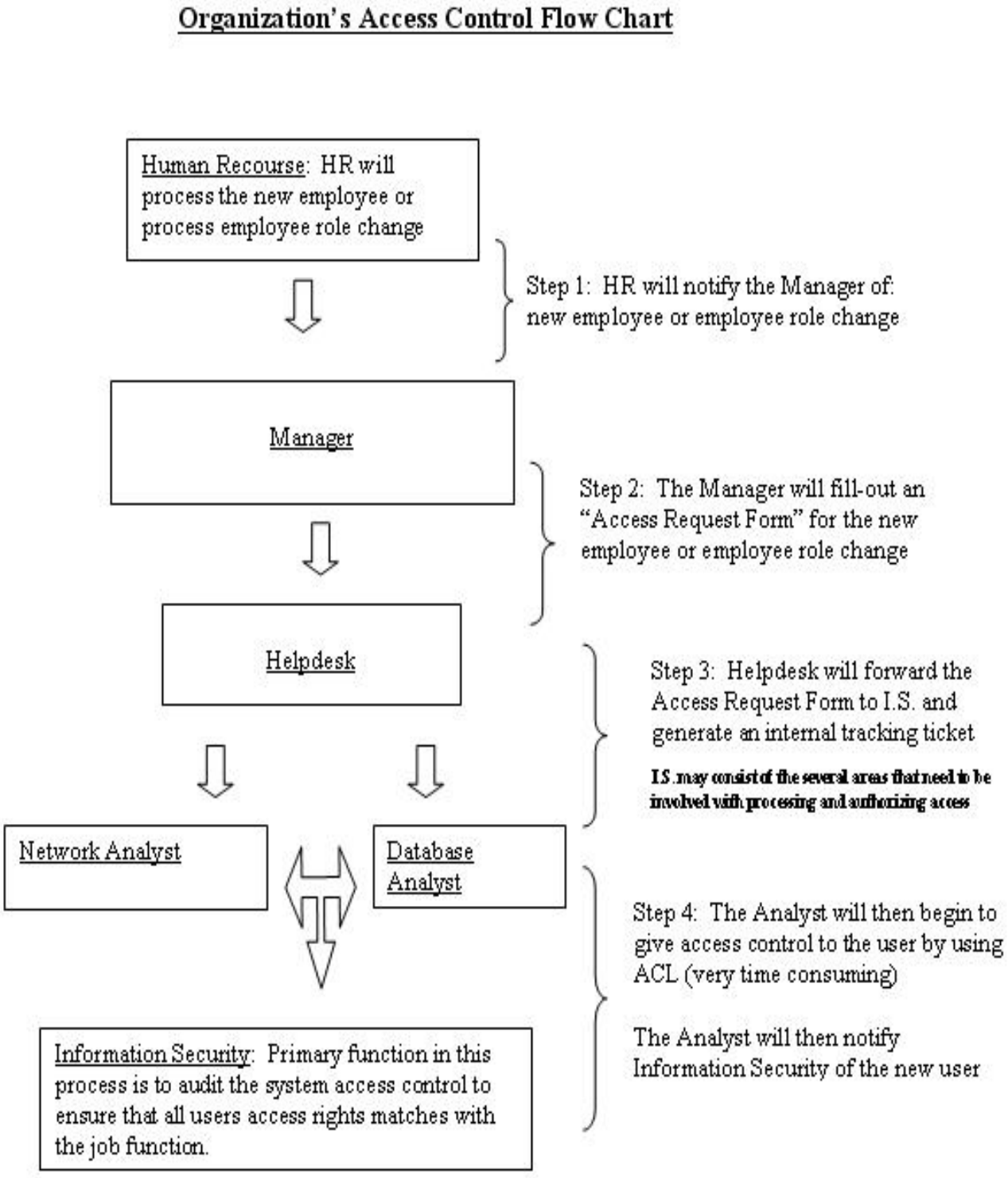
PROTECTED WHEN COMPLETED

FORM IS/4511 (2007 Apr)

The Manager is expected to check-off each individual resource that the Manager thinks the new user will need access to in order to perform that particular job function. The list also includes a selection that simply states "Client Access Similar to". What this means, is that the Manager can select an existing employee that may have a job function similar to the new employee. The existing employee's access permission will then be "cloned" to the new employee. Once this check-list is complete, the next step is to forward the SAR to the helpdesk. The Helpdesk Operator will then generate a request ticket for Microcomputer Services. There, the request ticket moves on to the Network Analyst and the Database Analyst, where it enters the permission granting stage. Depending on the individual's job function, the request may require both analysts to provide access to the information system. The analyst will look at the SAR and create a user ID based on a script that utilizes Windows Active Directory. The script will then prompt the analyst to assign the new user physical location and then the new user Organizational Unit. From there, all of the new user's access privileges are done manually based on the SAR check of resources or "Client Access Similar To" selection.

The process of changing or deleting existing employee access permissions is similar to that of a new employee. It is still based on the Systems Access Request checklist that is filled in by the authorizing Manager. The only difference is that if an employee changes positions, the analyst must remember to remove all of the employee's previous access before they add the new access permission. (See Figure 2 for Summary of the Organization's Access Control Flow Chart).

Figure 2.


Organization's Access Control Flow Chart
Human Recourse: HR will process the new employee or process employee role change
Step 1: HR will notify the Manager of: new employee or employee role change
Manager
Step 2: The Manager will fill-out an "Access Request Form" for the new employee or employee role change
Helpdesk
Step 3: Helpdesk will forward the Access Request Form to I.S. and generate an internal tracking ticket
I.S. may consist of the several areas that need to be involved with processing and authorizing access
Network Analyst
Database Analyst
Step 4: The Analyst will then begin to give access control to the user by using ACL (very time consuming)
The Analyst will then notify Information Security of the new user
Information Security: Primary function in this process is to audit the system access control to ensure that all users access rights matches with the job function.

2.2 Information Systems Auditing Process

There are two systems auditing processes that this Organization currently has in place. The first is the *daily* network auditing process and the second is the *annual* network auditing process. The daily network auditing process, conducted by the Information Security Branch, is performed daily because of the Organization's ever changing access needs. It starts once the access assignment to users is completed (usually the following day). A memo is forwarded from the Systems Analyst to the Information Security Branch for review and auditing. The purpose of this review is to ensure that the new user has been properly given the access to only what the new user needs to carry out their particular job function. Information Security will have to compare the new user's access permissions to that of the "clone" user or verify each of the permissions with the SAR Checklist. It is on a regular basis that the Information Security Branch must confirm their information with the authorizing Manager to ensure that the correct permissions are given. Even with this double verification, sometimes the permissions granted are still based on a "best guess" format depending on the user's job function.

In addition to the daily review, this Organization also conducts a yearly audit of every information systems resource. This is a lengthy and complicated process that involves a large number of high level management within the Organization. The process starts with Information Security generating a detailed report for each resource (resources may be an application or file structure). Each report will list every user who has access to it. The report is then given to the resource owner (usually a high level Manager). The resource owner will have to review the list to ensure that each user who is listed in the access group actually requires access to this resource to perform their respective job function. Given

that there are over 35 applications and approximately 59 top level folders and 828 second level folders, this process of auditing is extremely cumbersome, time consuming, and prone to error.

Here is an example of a typical day in this Organization in terms of access control changes (see Figure 3). There were 53 systems access changes made on June 25, 2007. Out of the 53 changes, 14 were in question by the Information Security Branch, which required further explanation and investigation.

Figure 3.

Example of Systems Access Control Changes for the Organization

Group Name	Description	Member Name	Administrato	TimeStamp
APP-EAS GLS	Security Enabled Local Group Member Added:	CN=APP-Gaming Licensing,OU=Global Groups,OU=Users - AGLC,DC=aglc,DC	CTheede	07-Jun-25 09:08:15
E-Clips	Security Disabled Universal Group Member Added:	CN=********,OU=Gaming Products and Services,OU=Users - AGLC,DC=aglc,DC	JAgustin	07-Jun-25 09:19:16
APP-EAS FinRev	Security Enabled Global Group Member Added:	CN=Financial Review 2,OU=Finance and Administration,OU=Users - AGLC,DC=	CTheede	07-Jun-25 08:53:02
Bingo Licensing Team	Security Enabled Global Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Casino Advisor Review Team	Security Enabled Global Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Casino License Team	Security Enabled Global Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Casino Operations Logistics T	Security Enabled Global Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Forensic Audit	Security Enabled Global Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
INTRANET - Bingo Results V	Security Enabled Global Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
PROSYS	Security Disabled Universal Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
GIN Users	Security Enabled Global Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Licensing St. Albert	Security Disabled Universal Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
GIN Authors	Security Enabled Global Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Forensic Audit North	Security Disabled Universal Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Forensic Audit Admin	Security Enabled Global Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Casino Revenue Assessment M	Security Enabled Global Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Bingo Facility	Security Enabled Global Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Due Diligence Workload	Security Enabled Global Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
APP-Stakeholder	Security Enabled Local Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
APP-Product and Pricing Stak	Security Enabled Global Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Licensing Supp-1	Security Disabled Universal Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Licensing Inspectors	Security Enabled Global Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Licensing and Charit	Security Disabled Universal Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Licensing Admin	Security Enabled Global Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Issues Briefing	Security Enabled Global Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Clientele	Security Enabled Global Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
First Nation Charities	Security Enabled Global Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
FinRev-Admin	Security Enabled Global Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Financial Review	Security Enabled Universal Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Licensing Support	Security Enabled Global Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
OPOL	Security Enabled Global Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Excluded Clerical	Security Disabled Universal Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
RICE-Admin	Security Enabled Global Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
E-Clips	Security Disabled Universal Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Investigations Inves	Security Enabled Global Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
VGER Reporting	Security Enabled Global Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Inspections - Policy Analysts	Security Enabled Global Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Investigations Admin	Security Enabled Global Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
WEBDB-Adobe PDF	Security Enabled Global Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
APP-Gaming Statistics	Security Enabled Local Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Due Diligence	Security Enabled Universal Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Due Diligence - Security	Security Enabled Global Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
Due Diligence-Casino Proposa	Security Enabled Global Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
INTRANET - Casino Results V	Security Enabled Global Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 08:18:50
First Nation Charities	Security Enabled Global Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 10:42:52
Casino License Team	Security Enabled Global Group Member Added:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	MNewton	07-Jun-25 10:42:52
APP-Licensing Restricted	Security Enabled Local Group Member Added:	CN=********,OU=Finance and Administration,OU=Users - AGLC,DC=aglc,DC=g	JHowse	07-Jun-25 10:55:28
APP-Product and Pricing Reac	Security Enabled Global Group Member Added:	CN=********,OU=Finance and Administration,OU=Users - AGLC,DC=aglc,DC=g	JHowse	07-Jun-25 10:57:21
APP-Whse Admin Audit	Security Enabled Global Group Member Added:	CN=********,OU=Finance and Administration,OU=Users - AGLC,DC=aglc,DC=g	JHowse	07-Jun-25 10:58:22
Finance Ex Whse	Security Enabled Global Group Member Added:	CN=********,OU=Finance and Administration,OU=Users - AGLC,DC=aglc,DC=g	JHowse	07-Jun-25 10:59:41
Finance ExWhse-St Albert	Security Enabled Global Group Member Added:	CN=********,OU=Finance and Administration,OU=Users - AGLC,DC=aglc,DC=g	JHowse	07-Jun-25 11:00:41
FinRev-Purchasing	Security Enabled Global Group Member Added:	CN=********,OU=Finance and Administration,OU=Users - AGLC,DC=aglc,DC=g	JHowse	07-Jun-25 11:02:24
APP-EAS Licensing Raffle	Security Enabled Universal Group Member Added:	CN=Licensing Raffle,OU=Distribution Lists,OU=Users - AGLC,DC=aglc,DC=go	CTheede	07-Jun-25 09:06:37
APP-EAS Licensing Raffle	Security Enabled Universal Group Member Added:	CN=Licensing Registrations,OU=Distribution Lists,OU=Users - AGLC,DC=aglc,	CTheede	07-Jun-25 09:06:37
APP-EAS GAIN	Security Enabled Global Group Member Added:	CN=Licensing Training,OU=Global Groups,OU=Users - AGLC,DC=aglc,DC=goa	CTheede	07-Jun-25 08:49:25
Reception	Security Enabled Universal Group Member Removed:	CN=********,OU=Regulatory,OU=Users - AGLC,DC=aglc,DC=goa,DC=ds	JAgustin	07-Jun-25 09:10:38
Lottery Field Srv	Security Enabled Global Group Member Added:	CN=********,OU=Gaming Products and Services,OU=Users - AGLC,DC=aglc,DC	WPrice	07-Jun-25 13:00:36

3 Issues with the Existing Process

After describing the information systems access and auditing process for this Organization, there are three areas of concern that have been identified by the Researcher. The first is *Systems Administration*, where the administration process is time consuming and there is no consistency in user permission assignment. The second is *Systems Security*, where there are policies to govern how access is granted; however, the process and procedure of provisioning userIDs are quite complicated. In addition, access is greatly dependent on the Manager's discretion which may lead to human error and "system access creepage". As a result, systems security may be at risk. Finally, is the *Auditing Process*, which has become increasingly complicated and time consuming.

3.1 Systems Administration

The existing Systems Administration process requires a large amount of time. When several key Managers and Information Systems Analysts were asked to provide information on how long, on average, it takes to add a new employee into the system using the current process, it was determined that the average amount of time to completely add a new user to the network varied from one to several days. The principal reason for this variance was that too many individuals were involved in the process and that with each step of the process being dependent on the previous step, a delay could occur at any given point. Upon closer examination, starting from the point of hire to when the information gets passed on to the Manager, the average time it takes for the Manager to fill out the checklist can vary anywhere from 20 minutes to days. This time variance is largely due to the complexity of the process. The Manager must take hours out of the day to review this checklist and to determine the appropriate resources for the new employee. Some Managers admitted that because this

process is so complicated and that they are unsure of the resources required, they tended to procrastinate or would just choose the "cloning" option. Once the checklist is complete and sent back to the Helpdesk, the Helpdesk Operator would take an average of 10 minutes to several hours to generate a request ticket for the Microcomputer Services. The Analyst(s) would then take an average of approximately 25 minutes to add a new employee to the network. Then, depending on the access requested, they would spend a varied amount of time verifying the new access permissions and perform the background work of checking to make sure it is the correct group and confirm to see if everything is functioning properly. Given that the Organization has over 35 applications and hundreds of folders, this is a very time consuming process. The Researcher believes that this process consumes too much time and that the process should be streamlined to reduce the amount of time an individual spends on access control.

3.2 Systems Security

The issue with this process is that granting access permissions is extremely subjective and not well standardized or controlled. For example, two individual users with the same organizational position and with the exact same job description may have different access permissions due to the fact that the authorizing Manager(s) may uses the SAR "cloning" for one and the SAR checklist for the other. In addition, the "cloning" process causes a great deal of security concerns for this Organization. As a case in point, if an individual user has the wrong access permissions that were not identified by the auditing process and those permissions are used for cloning for that specific job function, then as a result, the new user would have the same security risk as that posed by the original user. What this means is that the security risk is duplicated over and over again depending on how many users were cloned using this particular user. In addition to discrepancy in user permissions assignment at the

beginning, there is a concern of giving user access to a resource that they no longer need or that they should not have access to. This usually occurs when a user changes to a different job function. The current process is to remove all of the user's previous access before the new ones are added. Although this is the policy in theory, due to time constraints, this policy is not always a reality. The risk surrounding this is that the user now has access to segments of the network and resources that are not required for their particular job function. This is also referred to as "systems access creepage". "According to the most recent CSI/FBI Computer Crime and Security Survey, 98% of companies have firewall defenses in place and 97% have anti-virus software. Yet 52% of companies reported some type of security breach."[1] That is because these breaches are often forged internally.

> "In a growing or high-turnaround [organization], new people coming and going constitute a significant risk for corporate theft and mismanagement of network resources. One-third of all employees steal from their employers, and 75% of the time, this theft goes undetected. We are not just talking about pens and Post-Its here. Hackers have reportedly been hired at companies, stolen data from network segments they were unknowingly given access to, installed remote access trojans on their servers, and left."[2]

As a result, the Organization's Information Security Branch becomes forced to review access controls on a daily basis.

---

[1] http://www.scmagazineus.com/Beyond-the-firewall-Securing-your-internal-network/article/35559/, Sept. 19, 2007

[2] http://www.planetmagpie.com/news031406.aspx, Sept. 19, 2007

3.3 Auditing Process

Due to the inconsistency and lack of control with the Systems Administration process, Information Security has to spend a significant amount of time each day auditing each new user, as well as all the existing user job function changes, looking for "systems access creepage". This process consumes a large amount of time because it is a manual process. Information Security must look at each new user in the Active Directory to verify proper access measured against each userID to ensure that it is consistent with the SAR form. If there is a role change, then Information Security must ensure that the previous role permission is completely removed and that the new role is correctly granted. Since this is a manual process, it is indeed susceptible to human error.

The existing annual auditing process is extremely complex and time consuming due to the fact that each resource must be audited to ensure proper access control. Some of the resources will have hundreds of users in its access control list. Thus, to manually review each resource in detail is an extraneous and extensive process. However, because this Organization is a part of the Provincial Government, there is also the element of an external audit conducted by the Provincial Auditor. In previous audits, the Provincial Auditor suggested that the current process be reviewed and improved upon to make it easier to audit the Information Systems. An improved process with better mechanized controls needs to be created in order to simplify the current way of auditing the Information Systems.

4 Role-Based Access Control

As a result of the three areas of concerns that have been identified with this Organization's existing information systems access control process, the Researcher felt that exploring other access control methodologies would be beneficial to this Organization. In this section, the researcher will provide a brief and very simplistic description of the Role-Based Access Control Methodology, realizing that the RBAC Family of Models consists of many more complex layers. RBAC is an access control model based on the fundamental foundation that permissions are associated with roles, and that users are granted memberships in appropriate roles, thereby, acquiring the roles' permissions (e.g. see Ferraiolo, 2007, Ferraiolo & Sandhu, 2001 & RIT, 2002). In the context of an organization, roles are created for each job function and users are assigned and revoked role memberships based on the responsibilities of their job function. Roles add a level of abstraction between users and permissions, thus, simplifying the management of the many-to-many relationships between users and permissions. With RBAC, a single user can be associated with one or more roles, and a single role can have one or more user members. Hence, this will increase the overall ease of systems administration and may lead to an increase in the security of information systems (Li and Nita-Rotaru, 2003). Roles can be defined by examining the Organization's structure. In most large organizations, the roles are already established. They are broken down into divisions, branches, and specific individual roles. RBAC allows companies to specify and enforce security policies that map naturally to the organization's structure. However, RBAC does not have to align 100% to the organization's structure to be effective. The goal is to establish and create access provisions to as many of the Organization's roles as possible (80-20 rule).

5 Proposed Solutions

In the previous sections, the Researcher identified three areas of concern with the Organization's existing information systems access process. In this section, the Researcher will propose utilizing the Role-Based Access Control Methodology to address to each of these three areas of concern. As described above, there are several levels of hierarchy within the RBAC methodology; however, this research paper will utilize the most basic level of RBAC to propose solution to the three areas. The basic RBAC model was chosen to demonstrate that even at the most basic level, RBAC can improve this Organization's information systems access control. The most fundamental and basic concept of Role-Based Access Control is to create a role and assign access permission to resources based on the job function. In its simplest form, a role is nothing more than a security group with very specific access permission to resources that have been approved based on pre-established policy. The establishment of this policy must be a process that involves all levels management within the organization. Any modification to the role's access permission must follow the same process in order to prevent unauthorized changes.

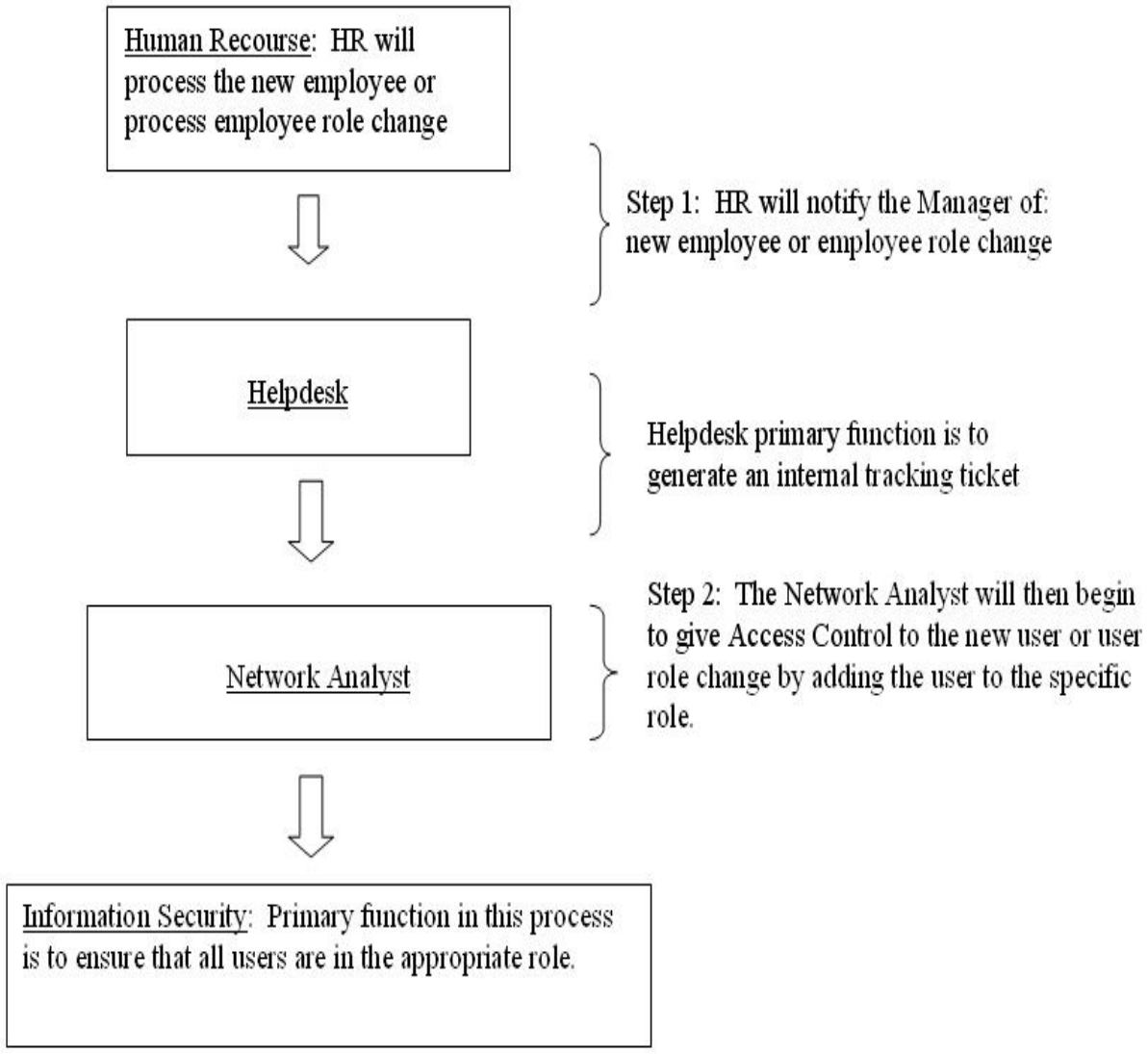
5.1 Simplified Systems Administration

The existing process in this Organization is full of administrative faults. RBAC would simplify systems administration by creating roles, which would be established and approved through policies, in accordance with the natural organizational chart. Thus, all of the security and access rights would already be built into the role. This simplifies the process for the Systems Administrator to be able to manage and control the systems access and removes the need to make discretionary changes. The new process would look something like the following, as compared to the existing process. First, the

Human Resources selection process would still apply. Then, once the new employee is hired, Human Resources would confirm with the Manager that the new employee will be operating in a specific role. The only additional information that would be requested from the Manager is if the individual requires any additional access outside of the role, which most of the time, this is not the case. Role policies would encompass everything the employee needs for their particular job function. This information would then be forwarded to the Helpdesk with a very specific role assignment. Helpdesk would generate a ticket for the Analyst to process. At this stage of the process, the amount of time any one individual would spend on the user's system access has already been reduced, due to the fact that no one individual needs to spend time further time evaluating the access request, since access for the role is already pre-defined. Therefore, all that is left is for the Analyst to do, is to simply add the new user to the existing role. As described in the RBAC methodology, the user will then have systems access based on their role selection. The Analyst does not have to spend the extra time manually adding on the new user to the Access Control List because the role has already been pre-established and approved.

In the case of an employee role change, the process is even simpler. The user is removed from the existing role, which means that the user no longer has access until they are added to the new role. As a result, there is less potential for "systems access creepage". The existing process described in this paper has more steps than what would be needed for efficiency and is also prone to errors due to the individualized, user-centric approach. By looking at the existing process flowchart, we can see how effectively RBAC has improved access control. As demonstrated in the Proposed Access Control Flow Chart (Figure 4), RBAC has reduced the total number of process steps.

Figure 4. Proposed Access Control Flow Chart with RBAC



In essence, what this means, is that Managers would no longer need to use the System Access Request Form, and it thereby eliminates second-guessing about what access a new user needs. In addition, the Manager is not required to reinvent access permissions for each new employee or role change in the Organization. However, RBAC is still adaptive enough to make custom access permission changes to

individual users without affecting the role itself. Overall, with RBAC, the Organization would simplify systems administration for everyone from the Manager, to the Helpdesk, to the Systems Administrators, and hence, to the Information Security Analysts.

One down side to this, however, is that it is actually difficult to accurately quantify how the proposed solution would save time for the Systems Administrator. Regardless, the concept of assigning a user to a role instead of assigning multiple individual access permissions to a single user, as in RBAC, is inherently more efficient.

5.2 Improved Systems Security

One of the identified issues with the existing process is Systems Security. As indicated, there is no consistency or well established process to provision access permissions. It is done simply by trying to give users access though the discretionary selection of resources by the user's Manager.

Since one of the main concepts of RBAC is to have predetermined roles that are pre-approved through policies by the Organization, it becomes very simple for a Systems Analyst to user assign permissions by simply placing the user in the appropriate role as indicated by the requesting Manager. The principal administrative action for Systems Administrators is to grant and revoke user's membership in and out of roles based on specific job functions. This is a stark contrast to the more conventional and less intuitive process of attempting to administer lower-level access control mechanisms directly on an object-by-object basis (Ferraiolo, 2007). Essentially, what this means is that human error would be greatly reduced by eliminating the manual process of granting individual access permissions to each user. This process would, in fact be "automated", in terms of granting

access permission. With users assigned to specific roles and permitted only to the rights and privileges of that role, "systems access creepage" would be reduced and strong systems security would be established.

5.3 Simplified Auditing Process

Although RBAC would not eliminate the daily audit of the information systems, what it does provide, is a more simplified and secure way of auditing user access. Instead of manually auditing a new user's individual access permission, Information Security would only have to ensure that the new user is assigned to the right role as requested by the Manager. This means that Information Security would not have to review each user and compare it to each resource to determine if access rights comply with policy. For existing users with a role change, Information Security would ensure that the user is removed from the old role and placed into the new role. The permission for that role would be a non-issue because it has already been pre-established. This new process would reduce the amount of time Information Security would have to spend on its daily network auditing.

As for the annual auditing process, the need for that would still exist. Information Security would simply need to review roles, to see that roles have the appropriate access rights based on policy instead of manually reviewing each resource. The auditing process would consist of confirming each role within the Organization to determine if it has been changed, replaced or removed. Each Manager would review each role under their authority and determine if the access permission is still appropriate for that particular role. If there are changes, it would be essentially simpler to make changes to a role that would propagate to all users who are in that role rather than to change all individual user access permissions.

6 Discussion

It is obvious that roles within an organization may not always be clear cut and simple. There are certain roles that are very complex and therefore, may not fit within the organization's conventional pre-established roles. The Researcher recognizes that the Role-Based Access Control Methodology may be able to define these certain roles; however, provisioning access for these roles may not be easy and "automated" like the other roles that are available within the organization. However, the 80-20 Rule can be applied to this. The goal of the Researcher is to identify and establish permissions for 80% of the Organization's roles. The other 20% can be done manually based on the specific needs of the role. Even with identifying only 80% of the organization's roles, it is still a more desirable approach to information systems access control.

There are, however, drawbacks with the RBAC Methodology that should be noted. The most significant is the initial background work to identify and establish permissions. This is one of the major reasons why organizations have not readily adapted the RBAC methodology. There is no doubt that adapting Role-Based Access Control to this Organization would be a complicated and time consuming process.

7 Conclusion

The growing demand for information technology forces an organization's information systems to also do the same. With so much traffic flowing through these systems on a daily basis: from user-to-user, from user-to-systems—both internal and external, it has become a complicated and time-consuming

process for everyone from managers to analysts to information security. This research paper identified a bona fide government organization and evaluated its information system security access control process. Through this evaluation, the Researcher discovered three areas of concern: *Systems Administration*, *Systems Security*, and the *Systems Auditing Process*. As proposed, the Role-Based Access Control Methodology was used as a solution for these issues. RBAC would simplify systems administration by creating roles with all of the access permissions already provisioned into the role. This creates a very simple process to manage and control system access merely by adding or removing a user to a specific role. Systems security would be enhanced with users' assigned to specific roles and permitted only to the rights and privileges of that role based on pre-existing policies instead of at the discretion of a manager. This would help reduce human error, and thus, "systems access creepage". However, as noted, RBAC would not eliminate the daily or the annual auditing process, but both auditing processes would be simplified by auditing roles instead of the less intuitive process of attempting to audit lower-level access control directly onto a resource. There is no doubt that adapting Role-Based Access Control to this Organization would be a complicated and time consuming process. However, as demonstrated, even in its simplest form, RBAC is an improvement over the existing process. And although change may initially be a daunting task, it would provide this Organization with the means to remain secure and adaptable in this dynamic and complex computer-dominated environment.

REFERENCES

[1] Covington, Michael et al, *Generalized Role-Based Access Control for Securing Future Applications*, College of Computing, Georgia Institute of Technology (February 2000).

[2] Ferraiolo, David, Kuhn, Richard & Chandramouli, Ramaswamy, *Role-Based Access Control*, 2nd ed. Norwood: Artech House, 2007.

[3] Ferraiolo, David et al, *Role-Based Access Control (RBAC): Features and Motivations*, NIST, U.S. Department of Commerce.

[4] Ferraiolo, David & Sandhu, Ravi et al, *Proposed NIST Standard for Role-Based Access Control*, ACM Transaction on Information and System Security, Vol. 4, No. 3 (August 2001).

[5] Li, Ninghui et al, *A Critique of the ANSI Standard on Role-Based Access Control*, CERIAS and Department of Computer Science Purdue University.

[6] RIT, *The Economic Impact of Role-Based Access Control*, NIST, Planning Report 01-1, 2002.

[7] Sandhu, Ravi, *The RBAC96 Model*, INFS 767, George Mason University, 2003.

[8] Sandhu, Ravi, Coyne and Edward et al, *Role-Based Access Control Model,* IEEE Computer, Vol. 29, No. 2 (February 1996).

[9] Shin, Dongwan, "*Role-Based Access Control for Trusted Management: Model, Processes, and Management*". University of Carolina, 2004.