One Employee and Several Applications: An Information Management Case Study

A. A. Elliott and G. S. Knight
Math and Computer Science, Royal Military College, Kingston, Ontario, Canada

Abstract - *In recent years, the use of Role-based Access Control (RBAC) has evolved within organizations such as the Government of Canada (GoC). However, it is not clear that existing on-boarding and off-boarding workflows have been influenced by the emergence of this technology. In this work, an Information Management (IM) case study is executed for one employee in the GoC. Results are summarized by human resource and staffing position and the advantages of on-boarding and off-boarding by staffing position are discussed. As the number of applications by employee increase, so too does the cost of the administrative processes. RBAC reduces the cost of administration at the authorization layer and its concepts can be applied at the authentication layer.*

Keywords: Information Management, Identity Management, Authentication, Role-based Access Control, Authorization.

1 Introduction

This Information Management (IM) case study is an investigation and analysis of the on-boarding and off-boarding procedures for one Government of Canada (GoC) employee and several applications with the following constraints:

- Each application (or dependent service) is required by the employee to complete the tasks associated with their staffing position.
- Each application (or dependent service) requires authentication – the successful entry of a username and password – to permit access.

Like the exterior of a new car, the authentication layer attracts much of the popular attention. Those who care how the car performs will spend several hours analyzing the detailed specifications of its engine and those who are charged with the responsibility of building the engine will agonize over minute details of its design and implementation in order to improve performance.

Role-based Access Control (RBAC) is the engine of IM systems. RBAC controls how well an IM system runs for each authenticated user. Once a user has successfully entered their username and password, RBAC controls what they can see and do in the system. If the engine has been poorly specified and implemented, users will not have access to the information they need to do their work or they may have access to information that they should not. That said, the key must be turned in order to start the engine and this study is primarily concerned with the authentication layer, where the username and password are considered the key to the IM system. Continuing with this analogy, the key management for one civilian employee in the GoC is analyzed to determine if the emergence of RBAC has influenced the on-boarding and off-boarding workflows.

As employees enter and exit GoC organizations there are a number of security challenges with respect to IM systems and RBAC as outlined in the Government Security Policy (GSP) and the Operational Security Standard: Management of Information Technology Security (MITS) [6][7]. However, this research is motivated by its desire to reduce the administration associated with Identity and Access Management (IAM). To that end, the following contributions are made; we provide detailed identity management information for a real world on-boarding and off-boarding scenario, we demonstrate that GoC employees are granted access to IM systems using administratively heavy person-based processes and we introduce an RBAC inspired solution for identity management in enterprise organizations [1][2][3].

The rest of this paper is organized as follows; section 2 provides background information for Information Management and Role-based Access Control, section 3 details the investigation and analysis conducted in this case study, section 4 briefly describes some related initiatives and section 5 concludes this work.

2 Background

The on-boarding process for a new civilian employee in the GoC may include a series of workflows that grant access to one or more applications. Likewise, the off-boarding process for a departing civilian employee in the GoC may include a series of workflows that remove access from one or more applications. Collectively, these processes are elements of a larger business process referred to as “employee turnover”.

2.1 Information Management

In its Policy on Information Management (IM), the GoC defines IM as "a discipline that directs and supports effective and efficient management of information in an organization, from planning and systems development to disposal or long-term preservation" [8]. An IM system can be a paper-based filing cabinet under lock and key or it can be a large centralized database of information. In the latter case, users might access this information through an application, using a "fat" client or "thin" client architecture, provided that they supply their username and password (Figure 1). After a user has successfully authenticated their identity, the application (or IM system) limits their access to authorized data with an access control mechanism such as RBAC. The terms IM system and application will be used interchangeably throughout this paper.

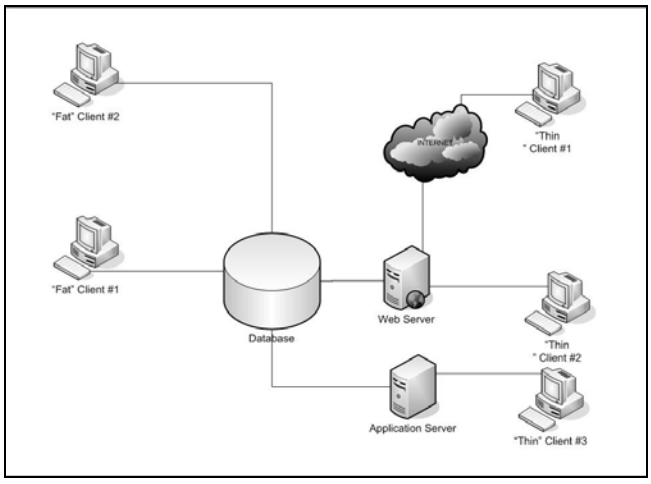

Figure 1. IM system architectures may include "fat" clients that connect directly to a database or "thin" clients that connect indirectly through application or web servers.

2.2 Role-based Access Control

The RBAC model was formally introduced by David F. Ferraiolo and Richard Kuhn at the 15th National Security Conference in October 1992 [4]. It has produced a standard, ANSI INCITS 359-2004, intended for software engineers designing products with role-based access control features [5].

A role is a semantic construct associated with permissions. Roles are created for the various job functions in an organization and users are assigned roles based on their responsibilities. Users can be easily reassigned from one role to another. Roles can be granted new permissions as new applications and systems are incorporated and permissions can be revoked from roles as needed. Role-role relationships can be established to implement broad policy objectives. This simplifies the effort required to manage security by reducing the number of administrative actions as illustrated in Figure 2. In case 1 there are five users and five tables. The total number of administrative actions is twenty-five when granting object permissions directly to users and ten when using the RBAC model – a savings of fifteen administrative actions. In case 2, the savings is eight thousand eight hundred administrative actions.

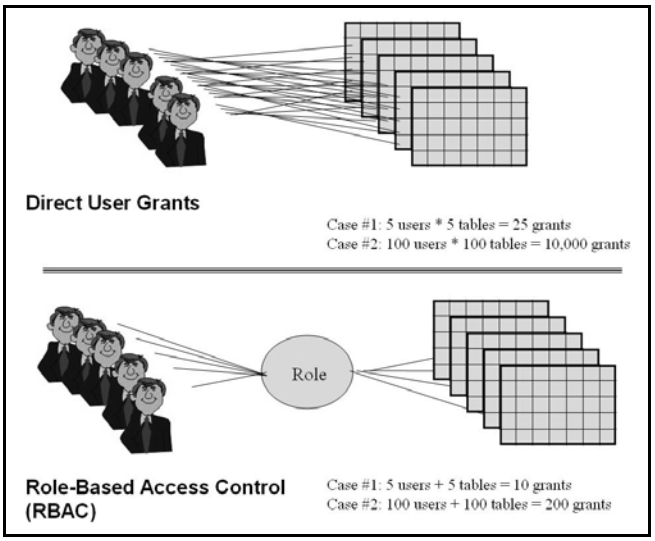

Figure 2. A classic example of the administrative actions required when granting object permissions directly to users and when using role-based access control. Case #1 is pictured and case #2 is included for emphasis.

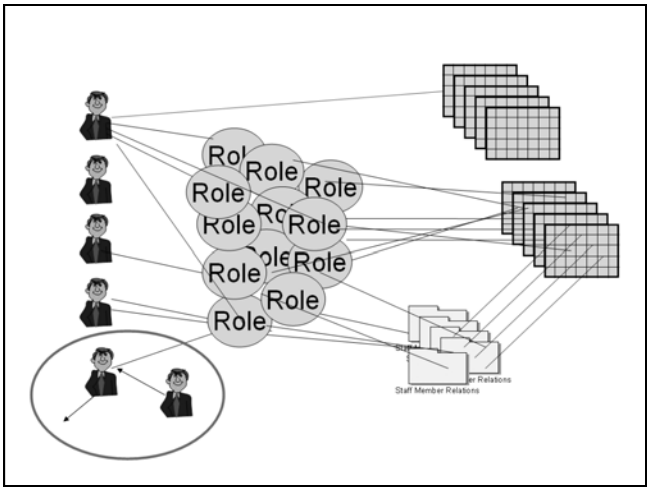

Figure 3. Employee turnover is a common event in enterprise organizations. An employee is leaving the organization and is replaced by a new human resource as circled at bottom left.

Although RBAC provides a solid foundation for managing security in an enterprise environment and Figure 2 is a "textbook" example, its utilization is often informal and ad-hoc in nature. A simplified example from an actual implementation might look like the one pictured in Figure 3 where the employee turnover process is occurring. This is a

practical example for one application so imagine how this might scale across several applications. As an employee leaves the organization, workflows must ensure that access is revoked from the applicable set of applications. Likewise, workflows must provision the new employee with access to the set of applications they require to fulfill the responsibilities of their staffing position.

Realizing that one GoC employee may have several username and password combinations, which is difficult to maintain in and of itself, and then considering that each one of these username and password combinations may be granted several roles provides some insight.

The following example uses arbitrary numbers:

- 1 GoC Employee
- 10 Applications or Services / Employee
- 5 Roles / Application

If one GoC employee has 10 applications or services requiring authentication and each account (i.e. username and password) has 5 roles, the number of roles being managed for one employee balloons to 50.

Under the assumption that more and more GoC employees are requiring access to more and more secure IM systems and the assumption that more and more IM systems are increasing the number of roles available to users in order to limit (or customize) access to information, one might conclude that the management of IM systems and roles is a growing concern for administrators.

3 Information Management Case Study

In the IM case study that follows, we provide detailed information for a real world on-boarding and off-boarding scenario. This information demonstrates that GoC employees are granted access to IM systems using administratively heavy person-based processes.

The participating organization is the Royal Military College (RMC) of Canada, a subunit of National Defence. The participating employee is Alice, the Administration Officer for College Information Services. After selecting the participating organization and employee, a listing of applications (or dependent services) was obtained (Table 1).

Then the workflows for the on-boarding and off-boarding of each of these services or applications were iteratively elaborated, captured and validated with the actors identified. This was done with simplified workflow diagrams using Microsoft Visio™. An example of the RMC Network, Mail and Active Directory on-boarding and off-boarding processes is pictured in Figures 4 and 5 respectively.

Table 1. A listing of Information Management applications (or dependent services) for employee Alice of the Royal Military College of Canada.

#	**IM system (or dependent service) required by employee Alice**
1A)	RMC Network Access
1B)	RMC Mail Account
1C)	RMC Active Directory Account
2	Defense Wide Area Network (DWAN) Account
3	Financial and Managerial Accounting System (FMAS)
4	Claims-X Web
5	Monitor Mass
6	College Information System Application (CISA)
7	Portal

After investigating the on-boarding and off-boarding workflows for each of the IM systems listed in Table 1, a presentation was made to the participating organization and actors on November 24th, 2008. There were one or more representatives from each of the 7 on-boarding and 7 off-boarding workflows captured in this study. Discussion topics included the following:

- Human resource versus staffing position based workflows
- The concept of capturing IM system requirements by staffing position
- The formalization of on-boarding versus the informalization of off-boarding
- Converting all on-boarding workflows to an electronic request for access model
- The combination of actors (approvers and enablers) and the perceived relationship with both security and flexibility

Feedback was used to determine the validity of the results, make additional modifications to the workflows and shape the “opportunities” presented in another meeting with the Computer Security Lab (CSL) group held on December 19th, 2008.

Tables are used to summarize the research results. Table 2 lists employee on-boarding details by human resource. Table 3 is an RBAC inspired solution for identity management in enterprise organizations which lists employee on-boarding details by staffing position. In this paper a staffing position is synonymous with a role as found in the RBAC literature.

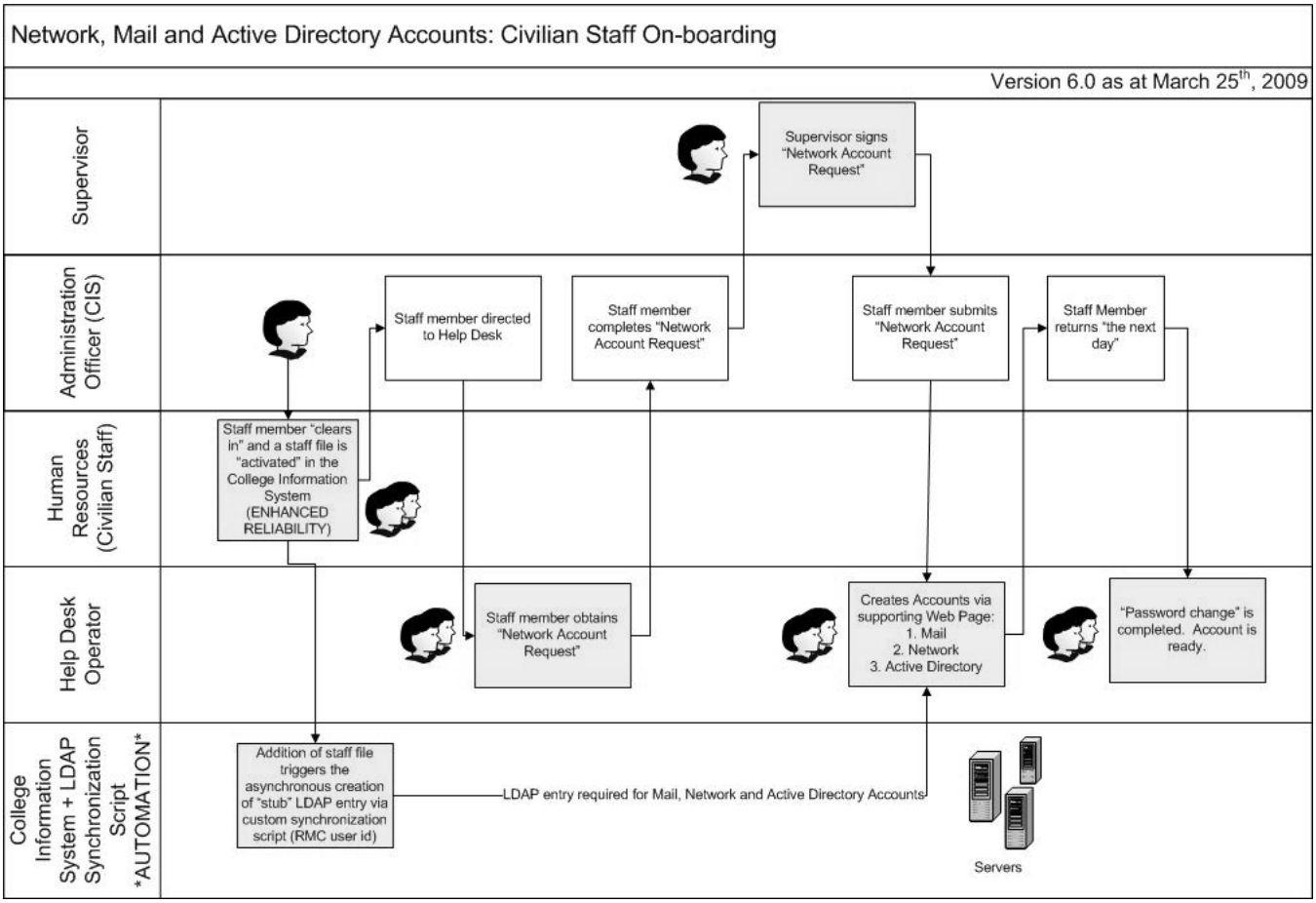

Figure 4. The RMC Network, Mail and Active Directory on-boarding workflow processes.

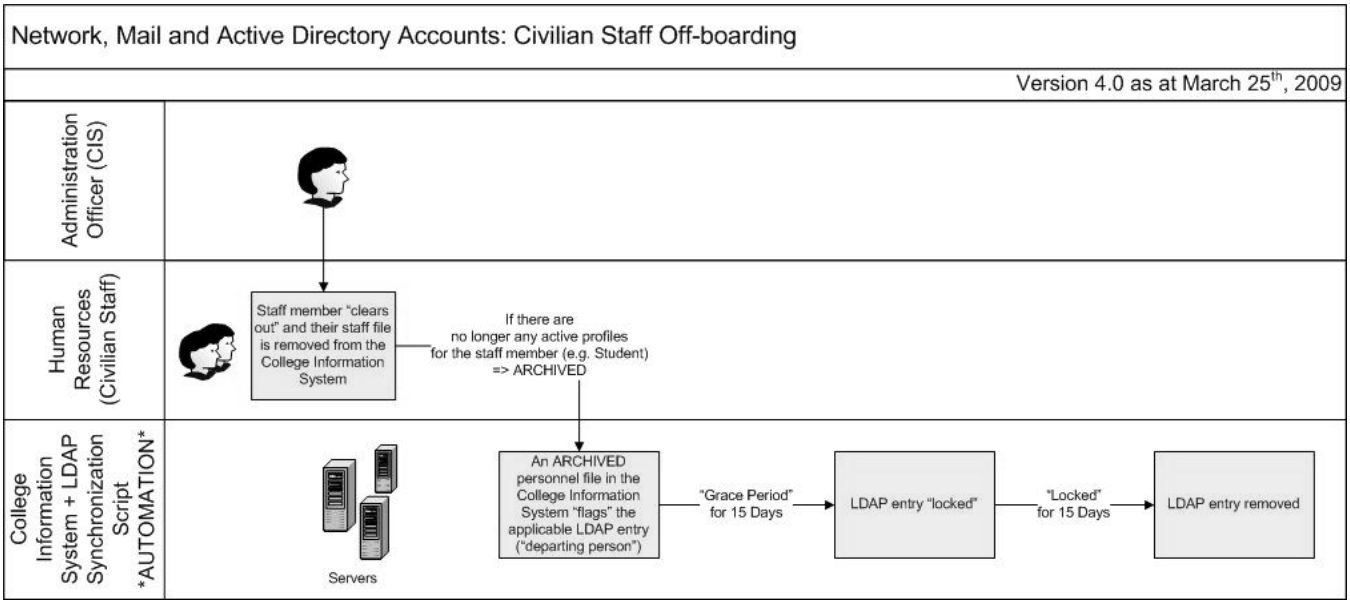

Figure 5. The RMC Network, Mail and Active Directory off-boarding workflow processes.

Table 2. On-boarding workflows by human resource include one or more approver and one or more enabler.

Employee	Service or Application	Approver(s)	Enabler(s)
Alice	(1A) RMC Network, (1B) Mail and (1C) Active Directory	Bob	Charlie or Dave (Form) and Charlie or Dave (Account)
	(2) DWAN	Bob and (Gregory or Homer)	Charlie or Dave (Form) Frank or notStaffed (Account)
	(3) FMAS	Bob and Eve and Isaac	Sarah (Form) Cindy (Account) Kim (Training)
	(4) Claims-X Web	Bob	Christine (Redirect) Barbara (Account)
	(5) Monitor Mass	Bob	Bob (Account)
	(6) CISA	Bob	Charlie or Dave (Trouble Ticket) Justin (Account)
	(7) Portal	Bob	Charlie or Dave (Mail Account)

Table 3. On-boarding workflows by staffing position include one or more approver and one or more enabler.

Employee	Service or Application	Approver(s)	Enabler(s) – Position Acronym
Admin Officer	1A) RMC Network, (1B) Mail and (1C) Active Directory	CIO	HDOP#1 or HDOP#2 (Form) and HDOP#1 or HDOP#2 (Account)
	(2) DWAN	CIO and (SCO#1 or SCO#2)	HDOP#1 or HDOP#2 (Form) and DWAN#1 or DWAN#2 (Account)
	(3) FMAS	CIO and Comptroller (RMC) and Comptroller (CFB)	FINO (Form) LACO (Account) TRCO (Training)
	(4) Claims-X Web	CIO	CXAD
	(5) Monitor Mass	CIO	CIO
	(6) CISA	CIO	HDOP#1 or HDOP#2 and CAD
	(7) Portal	CIO	HDOP#1 or HDOP#2

3.1 Human Resource Matrix

In Table 2, column 1 represents the employee – Alice – that is the subject of this case study. Column 2 lists the applicable service or application and columns 3 and 4 list the approvers and enablers by name. Of note, the on-boarding artifacts that enablers are associated with are included in brackets. This includes activities such as providing a paper based form or creating the account and notifying the employee.

3.2 Staffing Position Matrix

In Table 3, column 1 represents the staffing position – Administration Officer – that is the subject of this case study. Column 2 lists the applicable service or application and columns 3 and 4 list the approvers and enablers by staffing position. Of note, underlined position acronyms indicate vacant positions as at December 14, 2008.

The difference between Table 2 and 3 may appear trivial but consider the impact when Alice retires, for instance. The relations constructed in Table 2 no longer exist but the relations found in Table 3 remain when a new employee resources the Administration Officer staffing position.

As new employees enter the GoC, the cost of managing the on-boarding process may be very high due to the dynamics of informal human resource relationships like those found in this study. If Alice leaves the organization before the new employee arrives and Alice's supervisor has not thoroughly documented application requirements then the on-boarding process may prove administratively heavy due to the person-based processes in place.

Capturing IM system requirements by staffing position, as detailed in Table 3, facilitates the on-boarding process in enterprise organizations by formalizing access control requirements in an intuitive, scalable and dynamic framework. This framework can be used to fuel the automation of several activities including the four opportunities described in sections 3.3.1 and 3.3.3.

3.3 Analysis

Table 4 provides additional details for the on-boarding workflows investigated in this case study. Our analysis includes the following artifacts:

- Request for access method
- The combination of actors (approvers and enablers) and the perceived relationship with security and flexibility
- The capture of on-boarding statistics

3.4 Request for Access

One might question why paper-based forms are still required in 3 of the workflows listed in column 2 – Request for Access – of Table 4. If paper, pen and signature(s) are required to address legalities then there may be no alternative.

Table 4. On-boarding workflow artifacts are grouped to better visualize some of the similarities and differences for each of the 7 on-boarding processes analyzed. Note: This information relates to civilian employees with a Personal Record Identifier (PRI).

Service or Application	Request for Access	#Approvers	#Enablers	Combination of Actors Approval(s) * Enabler(s)	On-boarding Statistics
1A) RMC Network, (1B) Mail and (1C) Active Directory	Paper Form	1	(2)(2)	1*(2)(2)	No
(2) DWAN	Paper Form	(1)(2)	(2)(2)	(1)(2)*(2)(2)	No
(3) FMAS	Paper Form	(1)(1)(1)	(1)(1)	(1)(1)(1)*(1)(1)	No
(4) Claims-X Web	Email Request	1	1	1*1	No
(5) Monitor Mass	No Request	1	1	1*1	No
(6) CISA	Trouble Ticket	1	(2)(1)	1*(2)(1)	No
(7) Portal	No Request	1	2	1*2	No

Nevertheless, the paperwork could be produced from a Human Resources (HR) system where many of the informational fields such First Name, Last Name, Initials, etc. are pre-filled for the new employee.

This is the first opportunity for improvement. If a new employee does not have to complete paper-based requests for access then two immediate benefits are achieved. The first benefit is for the new employee who does not need to fill out the form and the second benefit is for the enablers (or system administrators) who do not need to decipher hand-written forms. In addition, the new employee might have validated the information on the form thus increasing the likelihood that the enabler and HR system has accurate information for them.

3.4.1 Combination of Actors

When summing the product of each cell in column 5 (Table 4), the combination of potential approvers and enablers during on-boarding totals 19 = 4 + 8 + 1 + 1 + 1 + 2 + 2. As at December 19th, 2008 there are 19 potential actor "paths" that an employee could traverse to obtain access to the 7 services and applications listed. 8 = 2 + 4 + 1 + 1 of the nineteen potential paths – or combinations of actors – includes the enabler, Dave, who is the supervisor for the recently vacated staffing position HDOP#2. The fact that the supervisor has assumed the duties of their subordinate is also nicely hidden in the staffing relationships of Table 3.

Continuing with column 5, and considering the DWAN on-boarding workflow. An employee requires the paper-based on-boarding form which is typically supplied by one of two employees (2 enablers). Next, the new employee must obtain the signature of the delegate for their department (1 approver) followed by the signature of one of the two Security Control Centre delegates (2 approvers). Finally, the new employee must deliver the signed form to one of the two DWAN administrators (2 enablers) who can create the account, test it and notify them on completion.

There are three comments that must be made with respect to the DWAN on-boarding workflow. First, not including the new employee themselves, it takes 4 GoC employees to make 1 DWAN account so one might argue that the workflow is administratively heavy. Likewise, the FMAS on-boarding process takes 5 GoC employees to make 1 FMAS account. Second, there are 8 possible combinations of actors that may partake in the creation of 1 DWAN account so one might argue that the DWAN on-boarding workflow is flexible. Conversely, one might argue that the FMAS on-boarding workflow is more secure because there is only 1 combination of actors.

Finally, consider how much time and energy (in distance traveled) that a new employee and/or supervisor expends obtaining, completing and delivering forms to obtain these accounts. This information has not been captured in this case study.

3.4.2 On-boarding Statistics

The second opportunity is the capture of on-boarding statistics. At present, it may be possible to determine the difference between employee start date and service or application account creation date – a measurement in days. This baseline could be compared to the statistics generated when making incremental change to the current workflow(s). As per column 6 of Table 4, none of the workflows record on-boarding statistics. Capturing statistics for the current state would provide a baseline for the introduction of incremental change.

The third opportunity is the introduction of a more formalized off-boarding procedure. It is curious, but perhaps not surprising, that organizations typically treat the off-boarding process much more informally then the on-boarding process. Some formalization for each of the off-boarding workflows might address the issue of orphaned user accounts.

The fourth opportunity for improvement is the capture of off-boarding statistics but it may be difficult to obtain a statistic for the current state. The employee end date could be compared to the account deletion date – a measurement in days – but most IM systems store metadata with the account itself implying that the deletion date would not be available after the account is removed.

4 Related Initiatives

Research was conducted in the commercial and academic solution domains and an interesting initiative from the Organization for the Advancement of Structured Information Standards (OASIS) termed Service Provisioning Markup Language (SPML) was deemed most relevant to this work. SPML is an XML-based framework for exchanging user, resource and service provisioning information between cooperating organizations and disparate systems [9]. SPML aims to achieve the following:

- Automated IT provisioning tasks: By standardizing the job of provisioning and making it easier to encapsulate the security and auditing requirements of provisioning systems, SPML pushes provisioning towards as much automation as possible.

- Interoperability between different provisioning systems: Different provisioning systems can now expose standard SPML interfaces to each other and interoperate with each other.

There are several commercial provisioning tools available for purchase but one interesting open source solution is Velo from Safehaus [10]. The framework used by Velo maps closely to the RBAC inspired, staffing position based framework presented in this paper and it is SPML v2 compliant.

5 Conclusions

In recent years, the use of Role-based Access Control (RBAC) has evolved within organizations such as the Government of Canada (GoC). In this work, we provide detailed information for a real world on-boarding and off-boarding scenario that is clearly not influenced by RBAC concepts. We demonstrate that the GoC employee in this study is granted access to IM systems using administratively heavy person-based processes. We introduce an RBAC inspired solution for identity and access management (IAM) by staffing position. Finally, we list opportunities for on-boarding and off-boarding improvements based on our solution.

6 References

[1] R. Crook, D. Ince and B. Nuseibeh. “Modeling Access Policies Using Roles in Requirements Engineering”, Information and Software Technology, 45 (14), pp. 979-991, Elsevier, 2003.

[2] A. Elliott and S. Thomas, “Administrative Role-based Access Control 2005”. Proceedings of the International Conference on Recent Trends in Information Systems (IRIS’06), Kovilpatti, India, January 6-8, 2006, pp. 454-465.

[3] S. Oh and S. Park, “An Improved Administration Method on Role-Based Access Control in the Enterprise Environment”, Journal of Information Science and Engineering, Volume 17, 2001, pages 921-944.

[4] D. Ferraiolo and R. Kuhn, “Role-based Access Control”, Proceedings of 15th NIST-NCSC National Computer Security Conference, Baltimore, MD, 13-16 October 1992, pp. 554-563.

[5] R. Sandhu, D. Ferraiolo and R. Kuhn, “American National Standard for Information Technology – Role Based Access Control”, ANSI INCITS 359-2004, February 3, 2004.

[6] Treasury Board of Canada Secretariat. (2002, February 1). Government Security Policy. Retrieved November 10, 2007 from http://www.tbs-sct.gc.ca/gs-sg/index_e.asp.

[7] Treasury Board of Canada Secretariat. (2004, April 14). Operational Security Standard: Management of Information Technology Security (MITS). Retrieved October 18, 2007 from http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328.

[8] Treasury Board of Canada Secretariat. (2007, July 1). Policy on Information Management. Retrieved April 5, 2009 from http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12452

[9] Verma, M. (2005, January 5) “Manage identities more effectively with SPML”. Retrieved December 21, 2008 from http://www.ibm.com/developerworks/xml/library/x-secspml1/

[10] Velo (Safehaus 2008, July 24). Retreived December 21, 2008 from http://docs.safehaus.org/display/VELO/Home