Economics of Access Control Policy Models for Identity Management
An Internet Survey Sponsored by
the National Institute of Standards and Technology (NIST)

Survey Instrument for Identity Management Professionals

Note: The survey is designed for the Internet;
This is a paper-based version that does not have skip logic or other features enabled

The National Institute of Standards & Technology (www.nist.gov) is sponsoring the following survey on the economics of access control policy models for identity management (IdM). The purpose of the survey is to understand how different access control models, like role-based access control (RBAC) and access control lists (ACLs), influence the efficiency and effectiveness of firms' IT and business workflows.

The survey is intended for active professionals in identity management, such as IT managers, senior systems administrators, and information security architects, for example. Question topics cover:

- business drivers underlying access control policy designs and decisions;
- routine provisioning;
- access control policy design, implementation, and maintenance; and
- compliance activities, including policy certification, permissions audits, and attestation.

The results will be used to inform strategic activities for IT standardization committees and organizations, as well as to report to the broader IT community on the economic costs and benefits of critical identity management activities.

As a participant in this study, you will receive a complimentary copy of this study's final report and economic analysis. You may respond anonymously, however anonymous respondents will not receive a copy of the study via email when it is released later in 2010.

It is expected that the survey will take between 15 and 30 minutes to complete, depending on your responses. Responses to this survey are confidential. At no time will any individual's name, any company or university name, their participation, or identifiable response be released to any third party, including NIST. The survey and analysis is being conducted by RTI International, a non-profit research institute. You may learn more about RTI's Technology Economics practice here.

Questions about the survey should be directed to Ross Loomis, Economist at (919) 541-6930 or rloomis@rti.org [US Eastern Time], or Alan O'Connor, Senior Economist and Project Director at (415) 848-1316 or oconnor@rti.org [US Pacific Time].

Click here to take the survey

OMB Control Number 0693-0033, Expiration Date 10/31/2012.
This survey contains collection of information requirements subject to the Paper Work Reduction Act (PRA). Notwithstanding any other provisions of the law, no person is required to respond to, nor shall any person be subject to penalty for failure to comply with, a collection of information subject to the requirements of the PRA, unless that collection of information displays a currently valid OMB Control Number. " Your response is voluntary and all data collected will be considered confidential. Public reporting for this collection of information is estimated to be 15 to 30 minutes per response, including the time of reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this estimate or any other aspects of this collection of information, including suggestions for reducing the length of this questionnaire, to the National Institute of Standards and Technology, 100 Bureau Drive, Stop 3220, Gaithersburg, MD, 20899-3220.

1. Respondent Profile
The following information will enable us to aggregate your responses with those of other respondents.

You may be complete this survey anonymously, however if you would like to receive a complimentary copy of the final report and analysis, your contact information must be provided. The opportunity to do so is at survey completion.

What is your job title?	
In what department or business unit are you principally employed (e.g., IT, security, risk management, accounting)?	
Which of the following best describes your organization's primary activity?	**<Drop down list of 2-digit NAICS>**
Which of the following best characterizes your organization's type?	**< Publicly-traded company, privately-held company, national government agency, state or regional government agency, academic institution, other>**
Approximately how many people were employed by your organization in 2009?	
Approximately how many accounts for intranet (e.g., employees and contractors) were maintained by your organization in 2009?	
What is your geographic location, if not USA?	

2. Overall Approach to Access Control Policy
Access control policies reflect organizations' current and legacy systems architecture, applications, business requirements, and workflows. Therefore, this question has two parts. The first part asks you to indicate the primary access control approach, or model, you use for key systems types and the number of users requiring access to those systems.

2a. In general, how would you characterize your approach, or model, to managing access for each of the following systems or application categories? (Hybrid approaches are common, and are addressed in the second part to this question.) Please select from the list of alternatives the response that **best** represents your access control approach for each systems group:

- **open access**, in which case all users in your organization have access;
- user- or group-based (via **access control lists** to which users are assigned by name or group affiliation),
- role-based (in which permissions are assigned to defined roles, and **roles** to users),
- rule-based (via if statements or other **rules** that determine access), or
- **not applicable**, including if you do not have systems or applications in this category

	Approach	Approximate number of users requiring access
Accounting and financial management systems	DROP DOWN Access Control Lists Open Access Roles Rules Not Applicable	
Electronic health record and health information systems		
Business process management systems		
Sales and customer relationship management systems		
Human resource information systems		
Directory services		
Identity management systems		
Purchasing, order management, and logistics systems		
Physical security services		
Network identity services		
Web services		
Enterprise database systems		

Comments?

2b.	In the second part of this question, you may indicate if, for each system category, you generally use a “hybrid” approach to your access control policy. For each system and application category, please indicate if – in general – you use a combination of roles, access control lists, and rules to manage access. Select all that apply.

	Access Control Lists	Roles	Rules	Open Access
Accounting and financial management systems				
Electronic health record and health information systems				
Business process management systems				
Sales and customer relationship management systems				
Human resource information systems				
Directory services				
Identity management systems				
Purchasing, order management, and logistics systems				
Physical security services				
Network identity services				
Web services				
Enterprise database systems				

Comments?

If they do not indicate roles in 2a or 2b, direct them to Question A3; if they do, proceed to Question 3.

3. Experience with Role-Based Access Control

You indicated that you use roles for managing at least some of your users' permissions. This section asks some basic questions about the types of systems for which roles are used at your organization, and whether you use "native roles" within an application or system, or is you use "enterprise roles" via an identity management solution.

Do you use roles that are native within applications? **Yes/No**

Do you use enterprise roles via an identity management solution that manages permissions for users across multiple applications and/or systems? **Yes/No**

Does your organization run an enterprise resource planning (ERP) system (i.e., Oracle, SAP)? **Yes/ No**

What were the main business and/or security drivers underlying your organization's use of roles?

Do you have any comments for us on the range of systems and applications for which you use roles, the effectiveness of using roles, or why roles are used for some systems and not for others?

4. Time Frame of RBAC Adoption

For each of the following time periods, please tell us the approximate number of users at your organization that had a least some of their permissions managed using roles. In the comments field, please offer any relevant insights. Your best approximation will suffice.

Periods:	**% Users with at least some permissions managed via roles**	**% of these users permissions managed via roles**
1999-2000	**%**	**%**
2001-2002	**%**	**%**
2003-2004	**%**	**%**
2005-2006	**%**	**%**
2007-2008	**%**	**%**
2009-2010	**%**	**%**

Comments?

5. RBAC Implementation Costs

The following questions ask you to reflect on the initial costs of designing and implementing a role-based access control policy model. Questions about policy maintenance and audit are asked in later sections. One FTE is approximately 2000 labor hours per year.

5a. Are you familiar with your organization's RBAC implementation costs and timeline? **Yes or No**

5b. If you are familiar with these costs, approximately…

How many months did the initial implementation of an RBAC model take? _____ **Months**

How many full-time equivalent (FTE) employees **from IT, Security, and Audit** were tasked with designing and implementing the RBAC policy? _____ **FTE**

How many full-time equivalent (FTE) employees **from business groups** were tasked with supporting RBAC policy design and implementation? _____ **FTE**

What was the approximate expenditure on third-party systems integration, services, role engineering, if any, *specific to implementing roles*? _____ **USD**

What were the approximate expenditures for software solutions or modules, *specific to implementing roles?* _____ **USD**

What were the approximate expenditures for hardware, *specific to implementing roles?* _____ **USD**

What are the approximate annual licensing or maintenance fees for your software solutions, if any, *specific to implementing roles?* _____ **USD**

Comments?

6. Routine Provisioning

The following questions explore the benefits of using roles for routine provisioning. The questions below address to issues: the frequency that common provisioning activities are conducted at your organization, and the downtime users experience when awaiting their permissions. Governance, risk, and compliance issues are addressed in subsequent questions.

6a. In a typical year, and for a typical pool of 1,000 users, approximately how many times does your organization perform the following activities? (For example, if for every 1,000 users, 200 have their permissions terminated, the response would be 200 times per 1,000 users. This implies a 20% turnover ratio.)

Assign existing permissions to new users _____ **Times per 1,000 users**

Change existing users' permissions _____ **Times per 1,000 users**

Establish new permission to existing users _____ **Times per 1,000 users**

Terminate permissions _____ **Times per 1,000 users**

Comments? _____

6b. When a new hire is made or a user changes roles, how much downtime does that employee experience while waiting for permissions to granted or changed (i.e., how many business hours is employee underentitled or unentitled?)

When RBAC is used _____ **Hours**

When ACLs are used _____ **Hours**

6c. How productive are users during this downtime? Please answer in percentage terms, where 100% indicates that the typical user is as productive as she or he would be without his or her permissions as with them. _____ **%**

Comments? _____

7. Access Control Policy Maintenance, excluding Governance, Risk, and Compliance

Access control policy maintenance has emerged as a business and IT These questions ask you to reflect on whether using roles has made access policy maintenance more efficient.

7a. Has the use of roles improved the efficiency of maintaining your organization's access control policy? **Yes or No**

Approximately, how many full-time equivalent (FTE) employees **from IT, Security or Audit** are tasked with maintaining your organization's access control policy, per year? _____ **FTE**

If roles were not used, by what percentage would this staffing allocation be higher, if at all? _____ **%**

Approximately, how many full-time equivalent (FTE) employees **from business groups** are tasked with maintaining your organization's access control policy, per year? _____ **FTE**

If roles were not used, by what percentage would this staffing allocation be higher, if at all? _____ **%**

Comments? _____

7b. Has your organization encountered any challenges with routine provisioning because of a lack of standardization in roles or specifications across different applications or systems? **Yes or No**

Comments? _____

8. Access Control Policy Governance, Risk, and Compliance
For the applications and IT systems whose access control policies are subject to audit and recertification processes, please provide estimate the number of users in the systems(s), how many times per year the system(s) are recertified, and estimates of the labor hours required for both IT and business managers to complete the recertification. [Regulations include Sarbanes-Oxley (SARBOX or SOX), FISMA, GLBA, HIPAA, FERC, PCI, and Basel II.]

	Regulation(s) requiring recertification	Number of users in system(s)	Number of system recertifications per year	IT Dept Time per recertification (labor hours)	Business Time per recertification (labor hours)
Accounting and financial management					
Business process management					
Sales and customer relationship management					
Human resource information					
Directory services					
Identity management					
Purchasing, order management, and logistics					
Information technology services					
Web services					

What are some of the challenges your organization has faced with IT audits and access control policy reviews? In what ways could standards organizations mitigate such challenges?

Comments? _____

9. Optional: Contact Information
Your contact information is required in order to receive a copy of the final report. Your responses and your contact information are confidential. As stated earlier, at no time will your name, affiliation, or any other identifiable response be provided to any third-parties, including the National Institute of Standards & Technology, which is sponsoring this analysis. lease also indicate if you would be willing to participate in a 15 to 20 minute follow-up interview about RBAC and the costs and benefits of using it for IT policies.

Respondent name (optional): _____

Affiliation (optional): _____

Telephone number (optional) _____

Email (optional): _____

Would you like to participate in a 15 to 20 minute, confidential follow-up telephone discussion about your responses? **Yes or No**

ALTERNATE QUESTION SET FOR NON-RBAC USERS

A3. Routine Provisioning

The following questions explore the benefits of using roles for routine provisioning. The questions below address to issues: the frequency that common provisioning activities are conducted at your organization, and the downtime users experience when awaiting their permissions. Governance, risk, and compliance issues are addressed in subsequent questions.

A3a. In a typical year, and for a typical pool of 1,000 users, approximately how many times does your organization perform the following activities? (For example, if for every 1,000 users, 200 have their permissions terminated, the response would be 200 times per 1,000 users. This implies a 20% turnover ratio.)

Assign existing permissions to new users _____ **Times per 1,000 users**

Change existing users' permissions _____ **Times per 1,000 users**

Establish new permission to existing users _____ **Times per 1,000 users**

Terminate permissions _____ **Times per 1,000 users**

Comments? _____

A3b. When a new hire is made or a user changes roles, how much downtime does that employee experience while waiting for permissions to granted or changed (i.e., how many business hours is employee underentitled or unentitled?)

_____ **Hours**

A3c. How productive are users during this downtime? Please answer in percentage terms, where 100% indicates that the typical user is as productive as she or he would be without his or her permissions as with them. _____ **%**

Comments? _____

A4. Access Control Policy Maintenance, excluding Governance, Risk, and Compliance

Access control policy maintenance has emerged as a business and IT. These questions ask you to reflect on the resource intensity associated with maintaining your organization's access control policy.

A4a. Has the use of roles improved the efficiency of maintaining your organization's access control policy? **Yes or No**

Approximately, how many full-time equivalent (FTE) employees **from IT, Security, and Audit** are tasked with maintaining your organization's access control policy, per year? _____ **FTE**

Approximately, how many full-time equivalent (FTE) employees **from business groups** are tasked with maintaining your organization's access control policy, per year? _____ **FTE**

Comments? _____

A4b. Has your organization encountered any challenges with routine provisioning because of a lack of standardization or common specifications across different applications or systems? **Yes or No**

Comments? _____

A5. Access Control Policy Governance, Risk, and Compliance
For the applications and IT systems whose access control policies are subject to audit and recertification processes, please estimate the number of users in the systems(s), how many times per year the system(s) are recertified, and estimates of the labor hours required for both IT and business managers to complete the recertification. [Regulations include Sarbanes-Oxley (SARBOX or SOX), FISMA, GLBA, HIPAA, FERC, PCI, and Basel II.]

	Regulation(s) requiring recertification	Number of users in system(s)	Number of system recertifications per year	IT Dept Time per recertification (labor hours)	Business Time per recertification (labor hours)
Accounting and financial management					
Business process management					
Sales and customer relationship management					
Human resource information					
Directory services					
Identity management					
Purchasing, order management, and logistics					
Information technology services					
Web services					

What are some of the challenges your organization has faced with IT audits and access control policy reviews? In what ways could standards organizations mitigate such challenges?

Comments? _____

A6. Familiarity with Role-Based Access Control (RBAC)
This analysis seeks to measure the economic benefits of using RBAC as opposed to access control lists (ACLs) for identity management. You indicated that you do not use roles for access control at your organization. Please answer the following questions.

Are you familiar with your organization's access control policy models?	**Yes or No**
Are you familiar with role-based access control or using roles for identity management?	**Yes or No**
Is your organization currently migrating towards using roles, or are you actively planning for using roles in the next 2 years?	**Migrating, Planning within 2 years, Have no Plans**
Do you believe that roles are relevant for your organization's business model?	**Yes or No**

Comments? _____

A7. Optional: Contact Information
<u>Your contact information is required in order to receive a copy of the final report</u>. Your responses and your contact information are confidential. As stated earlier, at no time will your name, affiliation, or any other identifiable response be provided to any third-parties, including the National Institute of Standards & Technology, which is sponsoring this analysis. lease also indicate if you would be willing to participate in a 15 to 20 minute follow-up interview about RBAC and the costs and benefits of using it for IT policies.

Respondent name (optional):	
Affiliation (optional):	
Telephone number (optional)	
Email (optional):	
Are you willing to participate in a 15 to 20 minute, confidential follow-up telephone discussion about your responses?	**Yes or No**