December 2010

2010 Economic Analysis of Role-Based Access Control

Final Report

Prepared for

National Institute of Standards and Technology
NIST Program Office
100 Bureau Drive
Gaithersburg, MD 20899

Prepared by

Alan C. O'Connor
Ross J. Loomis
RTI International
3040 Cornwallis Road
Research Triangle Park, NC 27709

RTI Project Number 0211876

RTI Project Number
0211876

Economic Analysis of Role-Based Access Control

Final Report

December 2010

Prepared for

National Institute of Standards and Technology
NIST Program Office
100 Bureau Drive
Gaithersburg, MD 20899

Prepared by

Alan C. O'Connor
Ross J. Loomis
RTI International
3040 Cornwallis Road
Research Triangle Park, NC 27709

Acknowledgements

This study benefited from the contributions of many individuals and organizations, especially the organizations that participated in our confidential survey and discussion series. In particular, the authors wish to thank several individuals in particular who reviewed draft material and participated in multiple rounds of interviews.

Many thanks to Kevin Kampman (Gartner), Rick Kuhn (NIST), David Ferraiolo (NIST), Gregory Tassey (NIST), Gary Daemer (Infusion Points), Michael Gallaher (RTI), Darran Rolls (SailPoint), Tim Weil (SecurityFeeds), and the Information Systems Audit and Control Association (ISACA).

Contents

Figures

Tables

EXECUTIVE SUMMARY

This study is a retrospective economic impact analysis of role-based access control (RBAC), one of the principal approaches for managing users' access to information technology resources.

For most organizations, networks, data, applications, and hardware and software systems are shared resources that users access to perform their duties. With access, however, comes the risk of intentional or unintentional misuse of or changes to systems and data, thereby threatening the integrity, confidentiality, and availability of an organization's information and its infrastructure.

IT managers wrestle with aligning engineered technology resources to business processes that are fluid and dynamic. Further, information privacy and internal-controls regulations have been enacted that specify access control policy characteristics with which systems must comply. And because organizations change faster than systems and face exogenous shocks like privacy regulations, legacy design issues generate friction between business operations and their counterparts in IT.

RBAC is arguably the most important innovation in identity and access management since discretionary and mandatory access control (Anderson, 2001; Bertino and Sandhu, 2005). It is the principle of controlling access entirely through "roles" created in the system that align to job functions (such as bank teller), assigning permissions to those roles, and then assigning those roles to employees, rather than using access control lists (ACLs) that assign permissions directly to users on an as-needed basis. A 2002 study completed by RTI International forecasted that RBAC could save U.S. organizations hundreds of millions of dollars per year (Gallaher, O'Connor, and Kropp, 2002).

ES.1 Study Scope and Objectives

The National Institute for Standards and Technology (NIST) has been at the center of RBAC's development for nearly 20 years, having developed RBAC conceptual models and standards in response to industry's needs and later transitioning to a standards role for the generic technology as software companies assumed the mantle of extending RBAC's capabilities into a broad array of products.

The study quantified economic benefits and costs, estimated the adoption of RBAC over time, and reviewed broader issues in identity and access management (IAM) for which using roles is advantageous. It offers an analysis of the economics of the myriad technological, business, and regulatory drivers underlying organizations' selection of which approach to access control is appropriate, given their organization's user base, staff turnover, workflow patterns, and regulatory considerations.

This study also assessed NIST's contributions to RBAC development by conducting a retrospective benefit-cost analysis to meet NIST's accountability goals for its expenditure of public funds in access control research.

ES.2 Overview of Role-Based Access Control

Information security requires an infrastructure that ensures people are who they say they are and provides users their appropriate level of access in order to conduct their assigned duties efficiently. Organizations must balance the benefits and costs of granting users IT permissions to arrive at the desired access control policy. They also must protect their IT resources from breaches of security, both accidental and intentional. In essence, access control policies specify who has access to what—and under what circumstances.

An organization's access control policy is a response to

- business drivers, such as lowering the cost of managing employees' permissions and minimizing the amount of time that users are without their necessary permissions;
- security drivers, ensuring information security, integrity, and availability; and
- regulatory drivers, such as when enterprises seek to comply with the Health Insurance Portability and Accountability Act (HIPAA) or the Sarbanes-Oxley Act of 2002 (often referred to as "SarbOx" or "SOX").

In organizations with few users or few resources to protect, maintaining an access control policy may be as straightforward as assigning access through an ACL—a list of users granted access. But for many organizations, especially medium and large ones, maintaining an access control policy requires a substantial dedication of resources because of the large number of users, objects, and systems. The more complex the IAM policies become, the more likely it is that they will contain errors from changes in regulations, implementation of new systems and policies, interactions among policies, or human error (Ni et al., 2009). Remedying such errors, combined with an inherently inefficient system structure, greatly increases IAM costs.

Although RBAC is not the perfect solution, it enables greater shared responsibility and more effective and efficient permissions management for IT and business operations. Principal advantages of RBAC include the following:

- More efficient access control policy maintenance and certification: RBAC facilitates and, relative to other approaches, reduces costs associated with governance, risk, and compliance (GRC) activities and through greater visibility of permissions assigned to users and easier verification of internal controls: access control policy maintenance, attestation of access control policies in place, certification of regulated information systems, and access control policy audits conducted by internal and external auditors.
- More efficient provisioning by network and systems administrators: RBAC reduces the costs of administering and monitoring permissions relative to ACLs and other antecedent access control models. RBAC allows for greater automation while

adhering to the specified access control policy. Changes to permissions are automated through role assignment rather than being manually assigned whenever a new user is hired, an existing user changes positions, or new applications or IT systems are adopted.

- Reduction in new employee downtime from more efficient provisioning: RBAC accelerates bringing "new" employees to full productivity. New employees are employees who have been recently hired or are existing employees placed in new positions within the organization. During this time period, these employees may be only marginally or partially productive because they are underentitled. These benefits greatly outweigh the benefits from greater efficiency in network and systems administrators' execution of provisioning tasks.
- Enhanced organizational productivity.
- Enhanced system security and integrity (see Figure ES-1).

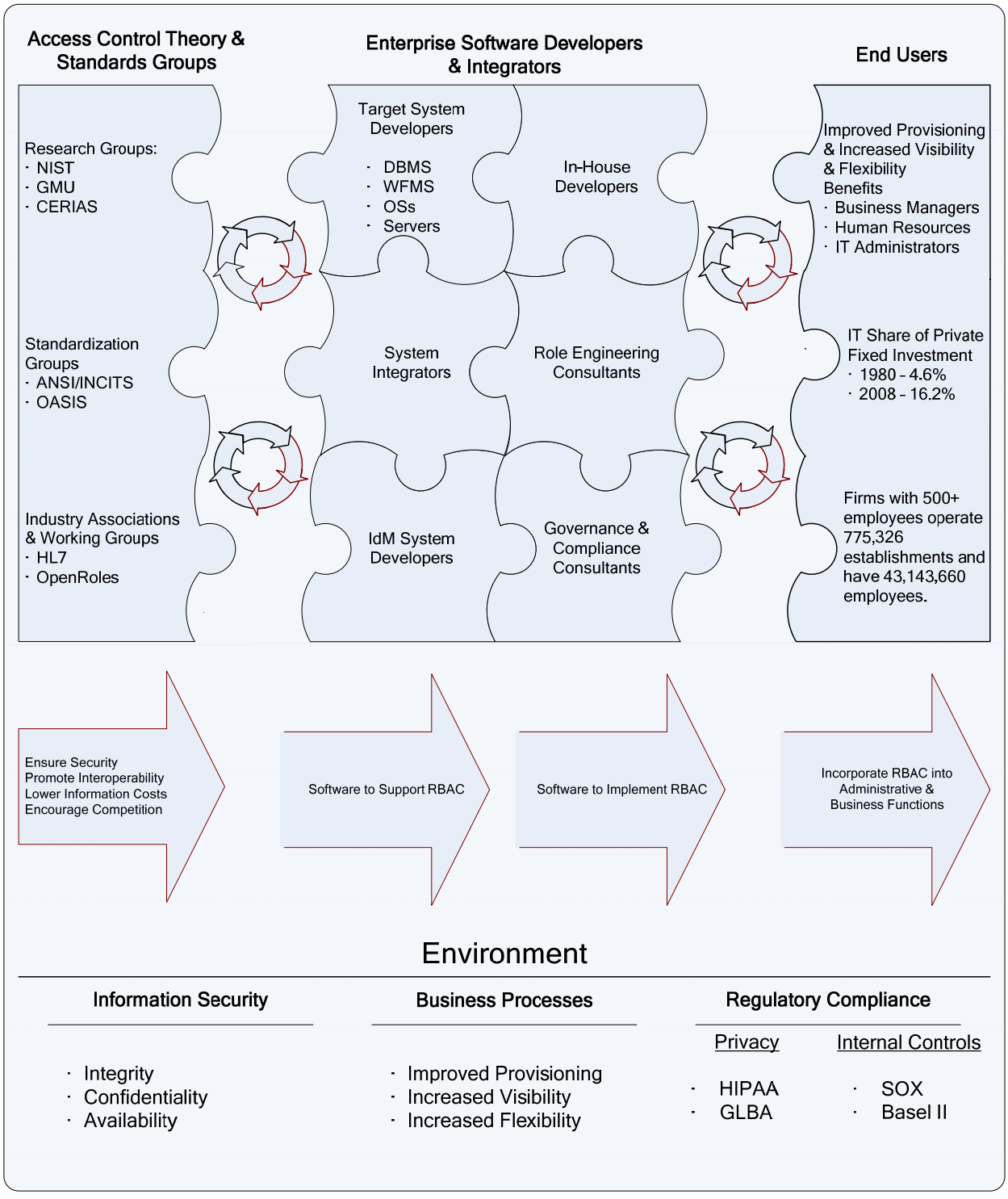
NIST developed and published a comprehensive RBAC model in 1992, providing the first RBAC technical specifications and formal description (Ferraiolo and Kuhn, 1992), followed by an expanded model (Ferraiolo, Cugini, and Kuhn, 1995). NIST, with Ravi Sandhu, at the time with George Mason University, proposed a standard for RBAC in 2000 (Sandhu, Ferraiolo, and Kuhn, 2000) that integrated the models of Ferraiolo and Kuhn (1992) with that of Sandhu et al. (1996). This proposal was revised in 2001 (Ferraiolo et al., 2001) based on comments received, and NIST drafted the final standard proposal and led the ANSI/INCITS RBAC standardization committee. ANSI/INCITS 359-2004, Role Based Access Control, was adopted in February 2004. The proposals and adopted standard largely eliminated the uncertainty and confusion about RBAC's utility and definition; it has served as a foundation for software product development, evaluation, and procurement specifications.

ES.3 Economic Analysis Approach Overview

Economic benefits for RBAC-adopting organizations were estimated relative to the use of groups, rules, and ACLs, net of ongoing operating costs and one-time adoption costs. A time series of benefits from 1992 through 2009 was calculated by estimating the rate of RBAC adoption and aggregating benefits across firms and industries. Reducing the time series of economic benefits by the annual costs incurred to develop RBAC and integrate its capabilities into software products yielded net economic benefit estimates.

One of the principal findings from the 2002 study was that NIST accelerated the introduction of RBAC by 1 year and reduced development costs. Therefore, benefits attributable to NIST were the difference between the time series of net benefits with and without these acceleration and cost-reduction effects. Thus, there are two bottom-line measures of interest: total net economic benefits of RBAC and net economic benefits of RBAC attributable to NIST.

Figure ES-1. RBAC Value Chain



Primary data were collected from stakeholders throughout the RBAC value chain, including a survey of IAM managers. A principal focus of early data collection was to engage each tier of the access control value chain—from developers through end users—to ensure that a complete taxonomy of economic benefit and costs categories was developed. Extensive discussions with IAM experts and managers were held to develop hypotheses about impact categories, review adoption drivers, and characterize adopting firms. This process was necessary to form the basis against which economic benefits might be quantified. Experts were from a diverse group of stakeholders, including technology research groups, government and university research centers, systems integrators, auditors, health systems, and large financial corporations.

One of the principal outcomes from these interviews was the development of a survey instrument for end users that RTI fielded with outreach support from the Burton Group (now part of Gartner), Information Systems Audit and Control Association (ISACA), and several IT blogs. Survey data were collected between July and September 2010. Companies responding to the internet survey and/or participating in in-depth interviews employed 2 million (4.5%) of the estimated 44.5 million people employed by organizations with more than 500 employees in 2010.

ES.4 Summary Findings and Analysis Results

The results from the survey and economic analysis fall into four overarching categories:

- trends in RBAC adoption and access control policy design;
- quantified economic benefits of RBAC (net of adoption costs), relative to alternate access control approaches;
- national economic impact estimates; and
- economic benefits attributable to NIST.

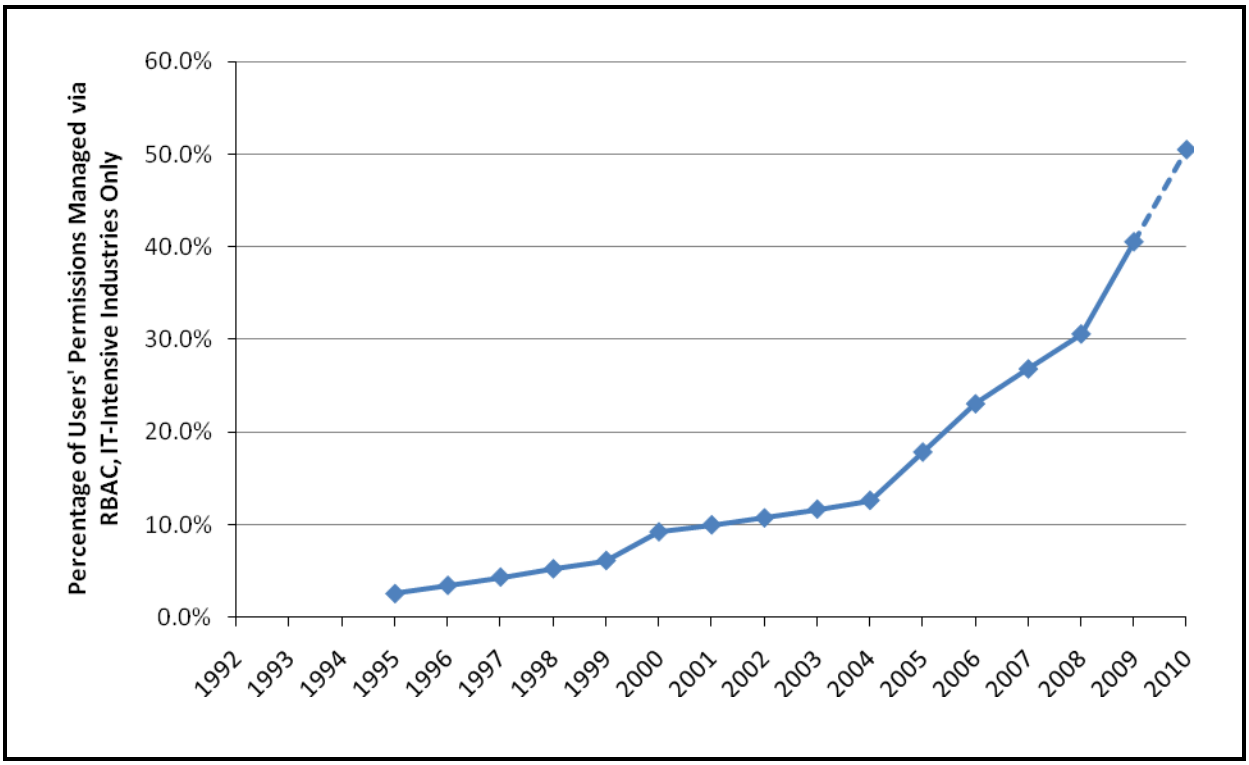
ES.4.1 Trends in Role Use and Access Control Policy Approaches

Survey results indicate that the use of roles has grown steadily since 1994, with the rate of RBAC adoption accelerating in 2004 and again in 2008. For 1995 we estimated just under a 4% penetration rate, growing to about 11% in 2002, 13% in 2004, and 41% in 2009. By the end of the time period illustrated in Figure ES-2, we estimate that just over 50% of users at organizations with more than 500 employees are expected to have at least some of their permissions managed via roles.

Over 80% of respondents reported that using roles improved the efficiency of maintaining their organization's access control policy (Table ES-1). These organizations were more likely to

- use roles that were native to applications and systems than they were to engineer their own roles (78% vs. 22%),

Figure ES-2. RBAC Adoption, 1992–2010



Note: Industries were defined by 2-digit NAICS code and included utilities; manufacturing; wholesale trade; retail trade; information; finance and insurance; professional, scientific, and technical services; educational services; health care and social assistance; arts, entertainment, and recreation; other services; and public administration.

Table ES-1. Adopters' Experiences with RBAC

Question	Yes	No
Has the use of roles improved the efficiency of maintaining your organization's access control policy?	84%	16%
Do you use roles that are native within applications?	78%	22%
Do you use enterprise roles via an identity management solution that manages permissions for users across multiple applications and/or systems?	54%	46%
Does your organization run an enterprise resource planning (ERP) system (i.e., Oracle, SAP)?	54%	46%
Has your organization encountered any challenges with routine provisioning because of a lack of standardization in roles or specifications across different applications or systems?	55%	45%

- use enterprise roles via an identity management solution that manages permissions for users across multiple applications and/or systems (54% vs. 46%), and
- encounter challenges because of a lack of standardization in roles or specifications across different applications and systems (55% vs. 45%).

As shown in Table ES-2, roles were most likely to be used as the primary access control mechanism for

- human resource information systems (56%);
- sales and customer relationship management systems (52%);
- purchasing, order management, and logistics systems (50%);
- accounting and financial management systems (50%); and
- business process management systems (44%).

Almost all organizations reporting hybrid approaches—such as roles and ACLs—reported using either roles as the primary mechanism and ACLs as the secondary one, or ACLs as primary followed by roles as secondary. As one respondent noted, "While we attempt to build RBAC controls, they tend to be implemented by using 'groups'; hence the separation of ACL and RBAC is difficult, as they tend to overlap."

In their remarks, respondents often expressed a preference for RBAC but were faced with the reality of business operations, applications, and systems that were inhospitable to it or for which RBAC would be counterproductive. The three most common barriers were the following:

- Certain combinations of user types, systems, and workflows do not lend themselves to effective management via roles.
- Legacy systems were not designed with sufficiently granular levels of authorization to be compatible with roles.

Table ES-2. Primary Access Control Mechanism Used, by Information System Category

System	ACLs	Roles	Rules	Attributes	Other
Human resource information systems	37%	56%	6%	2%	0%
Sales and customer relationship management systems	41%	52%	2%	4%	0%
Accounting and financial management systems	41%	50%	6%	2%	2%
Purchasing, order management, and logistics systems	41%	50%	7%	2%	0%
Business process management systems	42%	44%	7%	4%	2%
Enterprise database systems	43%	41%	10%	6%	0%
Electronic health record and health information systems	48%	34%	10%	7%	0%
Identity management systems	39%	34%	15%	7%	5%
Physical security services	50%	28%	9%	9%	4%
Directory services	49%	27%	10%	6%	8%
Network identity services	53%	22%	14%	6%	4%
Web services	51%	20%	14%	6%	8%

- RBAC implementation was perceived to be a significant investment of human resources, capital, and time, competing with other IT projects for limited resources.

Although many users and permissions fit well within static role definitions, there will always be a portion of users and permissions for which the costs of role definition and maintenance are prohibitive. Even a respondent whose organization has a highly centralized IAM solution reported that although "[r]oles are standard, other means are used when they do not easily interface with our centralized approach."

ES.4.2 Quantified Economic Benefits of RBAC

Economic benefits were quantified for:

- More efficient provisioning by network and systems administrators,
- Reduced employee downtime from more efficient provisioning, and
- More efficient access control policy maintenance and certification (see Table ES-3).

Provisioning benefits manifest in two ways: cost savings from provisioning activities by network and systems administrators and cost savings from reduced employee downtime. A small proportion of the economic benefits were related to provisioning activities conducted by network and systems administrators. Indeed, such labor savings amounted to less than 10% of the benefit accruing from reducing the period during which any given user is underentitled. For a hypothetical financial services firm with 10,000 employees, we estimate that RBAC saved only about $24,000 in IT department labor, but nearly $300,000 in reduced employee downtime, when national average wage rates are used.

Table ES-3. Quantified Economic Benefits of RBAC for Adopting Firms, per Employee (2009)

	Hours Saved per Employee, per Year	Average Loaded Hourly Wage Rate (2009)	Value per Employee per Year (2009)	Example Benefit for Financial Services Firm with 10,000 Employees (2009)
More efficient provisioning by network and systems administrators	0.035	$68.20	$2.38	$23,800
Reduced employee downtime from more efficient provisioning	0.55	$54.62	$29.80	$298,000
Quantified benefits from more efficient access control policy maintenance and certification				$1,107,400
IT staff	0.72	92.10	$65.95	
Business operations staff	0.45	98.94	$44.79	
Total quantified economic benefit			**$142.92**	**$1,429,200**

The principal source of economic benefit was from more efficient access control policy maintenance and certification. IT managers participating in interviews noted that they often expected provisioning to be the largest source of economic benefit, but regulatory compliance and governance policies increasingly point to broader benefits to consider, including enhanced insight into an organization's access control policy and more efficient maintenance of that policy.

Over 80% of survey respondents reported that roles have improved the efficiency of maintaining their organization's access control policy. The task of reviewing policies and maintaining the desired level of consistency across an organization's systems, functions, and groups requires close coordination between managers that engineer and maintain the IT infrastructure and the managers responsible for the business activities that use that infrastructure as a resource for doing their work.

One respondent reported the primary business driver for RBAC adoption was "to relate the granting of access to business roles which can be understood by authorizers, as opposed to function permissions, such as the mainframe transaction name, which are not understood by business managers." The hypothetical financial services firm would save about $1 million per year with RBAC.

Although roles do not eliminate the policy review and attestation process, they do make it easier to accomplish, especially when large numbers of employees fall within well-defined job functions for which roles are a particularly effective and efficient access control mechanism. We estimated that RBAC saved U.S. organizations $1.8 billion in 2009 from more efficient access control policy maintenance.

The most significant expense was role engineering and mapping of permissions and users to roles. Survey results about the costs of implementing RBAC varied significantly, with some organizations spending millions of dollars on custom systems, initiatives related to large-scale ERP implementations, and extensive systems integration services. In contrast, other organizations made use of native role capabilities within systems they were currently using.[1] The typical time required for implementation averaged about 18 months.

[1] To understand the costs of implementation, the survey included questions regarding expenditures on hardware, software, and third-party systems integration, services, and role engineering, as well as the level of effort for IT and business groups. To be included in our survey, expenditures were required to be unique to roles to avoid overestimating adoption costs. Research, development, and production of software products are among the most labor-intensive processes in the advanced technology sector. Although it is common for economic analyses to account for transfers of value by netting out product-related revenue, the labor intensity associated with developing and customizing RBAC products and product modules for the enterprise computing market is sufficiently high that expenditures on software products were included. We are overestimating the cost basis, but data were insufficient to resolve value added by different tiers in the value chain. Inclusion of these expenditures further reinforces that net economic benefit estimates and public investment performance measures are conservative.

On average, organizations with more than 500 employees expended $241.01 per employee to implement RBAC (Table ES-4):

- $201.65 per employee in labor expenditures for IT and business managers to design policies, map permissions and users to roles, and implement the new access control approach;
- $39.36 per employee for one-time nonlabor costs, principally software product expenditures and fees for systems integration services directly related to implementing roles; and
- $1.47 per employee for recurring licensing and maintenance fees.

ES.4.3 National Economic Impact Estimates

Before accounting for the adoption costs, we estimate that between 1994 and 2009 RBAC generated $11 billion in cost savings for American businesses.[2] Cost savings were offset by $5 billion in software and hardware expenditures, systems integration, and maintenance fees to yield economic benefits net of adoption costs of $6 billion (Table ES-5).

Table ES-4. Average RBAC Implementation Costs, per Employee

Category	Hours per Employee	Loaded Hourly Wage Rate (2009)[a]	Value per Employee (2009)	Average 18-Month Implementation Cost, Firm of 10,000 Employees (2009)
IT labor	0.75	$92.10	$69.37	$693,700
Business labor	1.34	$98.94	$132.28	$1,322,800
Nonlabor costs			$39.36	$393,600
Annual maintenance fees			$1.47	$14,700
Total	**2.09**		**$241.01**	**$2,410,000**

[a] For business labor, the value is for 2009 using the 2009 cross-industry average loaded hourly wage for management occupations. For IT labor, the value is the average for network systems administrators ($68.20) and computer systems managers ($116.00). Note: All dollar values have been adjusted to real 2009 dollars using the GDP implicit price deflator (BEA, 2009).

[2] Measured economic benefits are likely conservative because (1) only a subset of industries determined by survey responses, not all industries, was included in the analysis; (2) the minimum firm-size threshold included in the analysis was 500 employees; (3) wage rates used to monetize labor benefits were industry averages for all occupations and included lower-paid occupations that do not necessarily rely on IT for their positions; and (4) only the period of 1994 through 2009 was included in the time series of economic benefits because preceding and later periods could not be estimated accurately; therefore, future benefits of existing implementations were excluded.

Table ES-5. Time Series of Economic Benefits of RBAC

Year	Employees Managed Under RBAC (million)	Implementation Costs, ($ millions)	Benefits				Total Economic Benefits ($ millions)	Economic Benefit, Net of Implementation Costs ($ millions)
			More Efficient Provisioning ($ millions)	Reduced Employee Down Time ($ millions)	Access Control Policy Maintenance ($ millions)	Access Control Policy Certification ($ millions)		
1994	0.0	−152.6	0.0	0.0	0.0	0.0	0.0	−152.6
1995	1.0	−111.1	1.1	10.3	46.5	0.0	57.8	−53.3
1996	1.4	−75.3	2.6	27.7	109.3	0.0	139.5	64.2
1997	1.8	−75.6	3.4	34.8	141.9	0.0	180.1	104.5
1998	2.1	−83.9	4.1	42.0	174.4	0.0	220.6	136.6
1999	2.5	−225.5	5.0	48.6	209.3	0.0	262.9	37.4
2000	3.9	−140.4	7.2	68.2	301.4	0.0	376.7	236.3
2001	4.3	−62.8	9.4	87.8	390.9	0.0	488.1	425.2
2002	4.5	−91.2	10.1	103.2	445.7	0.0	559.0	467.8
2003	4.9	−109.3	10.9	111.7	491.8	8.6	623.1	513.8
2004	5.4	−414.8	12.1	120.7	543.2	9.5	685.4	270.6
2005	7.7	−565.9	15.2	150.3	683.0	11.8	860.3	294.3
2006	10.1	−471.0	20.7	205.0	938.6	16.0	1,180.4	709.4
2007	11.9	−420.6	25.9	256.1	1,186.7	20.0	1,488.7	1,068.1
2008	13.6	−894.4	30.1	301.2	1,396.9	23.3	1,751.6	857.2
2009	18.0	−1,094.4	37.7	379.2	1,752.1	29.1	2,198.2	1,103.7
Total		**−4,988.9**	**195.5**	**1,946.6**	**8,811.8**	**118.3**	**11,072.3**	**6,083.4**

Note: Industries were defined by 2-digit NAICS code and included utilities; manufacturing; wholesale trade; retail trade; information; finance and insurance; professional, scientific, and technical services; educational services; health care and social assistance; arts, entertainment, and recreation; other services; and public administration. All dollar values have been adjusted to real 2009 dollars using the GDP implicit price deflator (BEA, 2009).

ES.4.4 Economic Benefits Attributable to NIST

To estimate net economic benefits attributable to NIST, a counterfactual economic analysis incorporating lower R&D efficiency for software developers and a 1-year delay in RBAC development, and therefore adoption, simulated how net economic benefits would accrue without NIST's involvement. Baseline economic benefits include NIST's impact on R&D efficiency and the timing of RBAC adoption. Software developers' R&D costs were estimated to be $69 million (see Chapter 5), yielding net economic benefits of $6,083 million (Table ES-6).

Delaying RBAC's development by 1 year and increasing the development cost under a scenario in which NIST did not participate in RBAC development has the effect of decreasing net benefits from $6,083 million to $4,904 million, a difference of $1,110 million (Table ES-6).

Table ES-6. Net Economic Benefits of RBAC and Net Benefits Attributable to NIST

	Baseline Net Benefits of RBAC			Net Benefits without NIST				
Year	R&D Expenditures ($ millions)	End-User Benefits ($ millions)	Net Benefits ($ millions)	R&D Expenditures ($ millions)	End-User Benefits[a] ($ millions)	Net Benefits ($ millions)	NIST Expenditures ($ millions)	Net Benefits Attributable to NIST ($ millions)
1992							−0.1	−0.1
1993							−0.1	−0.1
1994		−152.6	−152.6				−0.2	−152.9
1995		−53.3	−53.3		−152.6	−152.6	−0.6	98.7
1996	−6.24	64.2	58.0		−53.3	−53.3	−0.6	110.7
1997	−6.24	104.5	98.2	−6.80	64.2	57.4	−0.5	40.3
1998	−6.24	136.6	130.4	−6.80	104.5	97.7	−0.4	32.3
1999	−6.24	37.4	31.2	−6.80	136.6	129.8		−98.7
2000	−6.24	236.3	230.1	−6.80	37.4	30.6		199.4
2001	−6.24	425.2	419.0	−6.80	236.3	229.5		189.4
2002	−6.24	467.8	461.6	−6.80	425.2	418.4		43.2
2003	−6.24	513.8	507.6	−6.80	467.8	461.0		46.5
2004	−6.24	270.6	264.3	−6.80	513.8	507.0		−242.7
2005	−6.24	294.3	288.1	−6.80	270.6	263.8		24.3
2006	−6.24	709.4	703.2	−6.80	294.3	287.5		415.7
2007		1,068.1	1,068.1	−6.80	709.4	702.6		365.5
2008		857.2	857.2		1,068.1	1,068.1		−210.9
2009		1,103.7	1,103.7		857.2	857.2		246.5
Total	**−68.7**	**6,083.4**	**6,014.7**	**−74.8**	**4,979.6**	**4,904.8**	**−2.6**	**1,107.3**
	NPV of net benefits ($ millions, base year = 2000)							**835.0**
	Benefit-to-cost ratio							**249**

Note: All dollar values have been adjusted to real 2009 dollars using the GDP implicit price deflator (BEA, 2009).

NIST's RBAC activities represented a cost to the government of $2.6 million during the 1990s.[3] Reducing the difference in net economic benefits by $2.6 million in public expenditures yields economic benefits attributable to NIST. We estimate that economic benefits of RBAC attributable to NIST are $1,107 million. Applying the 7% real social discount rate specified by the Office of Management and Budget (OMB) yields a net present value of $835 million (base year = 2000)[4] and a benefit-to-cost ratio of 249.

[3] Although NIST's researchers were engaged in standardization and research activities after 2000, these costs were not tracked closely because they were incurred on an ad hoc basis and were not considered sufficiently material by NIST management to warrant the expense of formalized reporting. The majority of costs incurred between 1999 and 2009 were for the RBAC support Web site, conference and travel support related to participation in standardization activities, and labor effort of less than 0.2 FTE per year.

[4] A base year of 2000 was selected to correspond to the base year uses in the 2002 prospective economic analysis and to reflect that, although the generic technology was developed in 1992, the infratechnology aspects (such as the INCITS 359-2004 standard) of NIST's contributions were more recent.

1. INTRODUCTION

This study is a retrospective economic impact analysis of role-based access control (RBAC), one of the principal approaches for provisioning users' permissions for information technology resources. Although the process of assigning, modifying, or terminating permissions seems mundane, it is a one of the most important activities within the core IT management function.

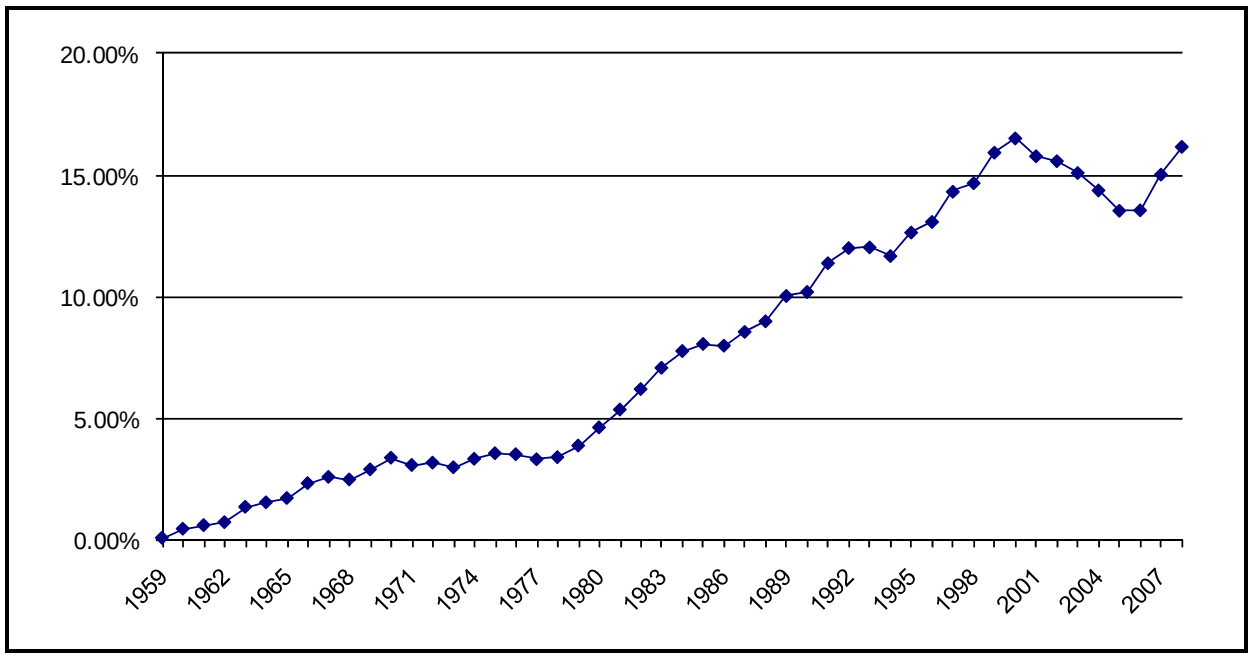
For most organizations, networks, data, applications, and hardware and software systems are shared resources that users access to perform their duties. Over the past 30 years, advances in the data processing, organization, and communication capabilities of information technology have dramatically transformed the way in which organizations function. Software, computers, and peripheral equipment grew from 4.6% of U.S. private fixed investment in 1980 to 16.2% in 2008 (about $348.3 billion, 2009$) (Figure 1-1). With access, however, comes the risk of intentional or unintentional misuse and changes to systems and data, threatening the integrity, confidentiality, and availability of an organization's information and its infrastructure.

IT managers wrestle with aligning engineered technology resources to business processes that are fluid and dynamic. Further, information privacy and internal-controls regulations have been enacted that specify access control policy characteristics with which they must comply. And because organizations change faster than systems and face exogenous shocks like privacy regulations, legacy design issues generate friction between business operations and their counterparts in IT.

RBAC is arguably the most important innovation in identity and access management since discretionary and mandatory access control (Anderson, 2001; Bertino and Sandhu, 2005). RBAC is the principle of controlling access entirely through "roles" created in the system that align to job functions—such as bank teller—and assigning permissions to those roles and then those roles to employees, rather than using access control lists (ACLs) that assign permissions directly to users on an as-needed basis. A 2002 study completed by RTI International forecasted that RBAC could save hundreds of millions of dollars per year (Gallaher et al., 2002).

Using roles has the advantage of streamlining the provisioning process, gaining insight into how permissions are and have been allocated, and, for some organizations, helping to more closely align their IT systems to their organizational structure and workflow. Although ad hoc uses of RBAC occurred as early as the 1970s, RBAC was not formalized or systematized until the National Institute of Standards and Technology (NIST) offered a formal definition in 1992. Although RBAC is not the perfect solution, it enables greater shared responsibility and more effective and efficient permissions management for IT and business operations.

Figure 1-1. Growth in Software and Computer Equipment as a Share of U.S. Private Fixed Investment



Source: Bureau of Economic Analysis. "National Income and Product Accounts: Table 5.3.5. Private Fixed Investment by Type." <http://www.bea.gov/national/nipaweb/Index.asp>. Accessed April 14, 2009; last revised March 26, 2009.

The purpose of this 2010 update is to return to the economic analysis of RBAC and assess RBAC's economic benefits retrospectively, review current trends in access control, and compare the 2002 study's forecast to actual results. This study quantifies economic benefits and costs, estimates the adoption of RBAC over time, and reviews broader issues in identity and access management for which using roles is advantageous. It is also an analysis of the economics of the myriad technology, business, and regulatory drivers underlying organizations' selection of which approach to access control is appropriate, given their organization's user base, staff turnover, workflow patterns, and regulatory issues. This study also assesses NIST's contributions to RBAC development, offering a retrospective benefit-cost analysis to meet NIST's accountability goals for its expenditure of public funds in access control research.

1.1 Access Control and Information Security

The term "access control" refers to an organization's policy for authorizing access in a networked environment, the mechanisms that provide and enforce the access control policy, and the models on which policies and mechanisms are based.

Access control is an integral element of information security, a concept that is understood in theory but that becomes elusive as discussions transition from the conceptual level to nuanced topics in computer science and network engineering. Yet a strong capability to articulate an

organization's information security needs and gauge risk tolerance is essential for determining how access should be managed.

The U.S. Code defines information security as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide

(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(C) availability, which means ensuring timely and reliable access to and use of information" (U.S.C., 2006).

Events related to unauthorized access that generate substantial losses are almost always related to the violation of one of these three requirements. Improper divulgence of confidential information can cause significant harm to individuals, an organization, or to our nation.

The confidentiality of medical information allows patients to be fully honest with doctors, enabling proper diagnosis and treatment. Internal controls protecting this doctor–patient confidentiality must be in place to yield the benefits of electronic health records. In another context, the release of confidential business information can jeopardize a company's competitive advantage in the marketplace in many ways, such as revealing product development plans or leaking details of a planned acquisition prior to its planned public disclosure.

Integrity refers to the maintenance of information accuracy. If a user has permission to write to a database when she only needs to read information in the database, then there is the potential for an accidental modification of the information. In January 2008, it was learned that a securities trader at Société Générale had a combination of permissions that allowed him to create fictitious trades. The fraud resulted in a €4.9 billion ($7.2 billion) trading loss for the French banking group (PriceWaterhouseCoopers, 2008).

In contrast to confidentiality and integrity, availability refers to whether information can be used when accessed. If an object, system, or network with business-critical information crashes, through intentional or unintentional disruptions, the result may be productivity losses for an organization until it is brought online.

1.2 NIST's Role in the Emergence and Development of Role-Based Access Control

The development of RBAC represented a focused effort on the part of NIST to develop a standardized model for access control that met industry requirements and relied on clearly defined terms and concepts. RBAC has been praised for "its scalability, flexibility, ease of

administration, and usability from the lowest operating system to the highest software application level" (Leahu et al., 2008, p. 386).

In 1992, NIST researchers David Ferraiolo and Richard Kuhn published the first comprehensive RBAC model, providing foundational technical specifications and formal descriptions (Ferraiolo and Kuhn, 1992). Later working with Ravi Sandhu, at the time of George Mason University, NIST supported development and adoption of RBAC by conducting research on specialized RBAC topics, sponsoring symposia, developing standards, and providing proof-of-concept designs and implementation support to software developers and standards committees.

From an economics perspective, NIST's contributions to RBAC fall predominantly in two general categories: generic technologies and infratechnologies (Tassey, 1997, 2007; Gallaher et al., 2002). Generic technologies provide a technology base for RBAC market applications, and infratechnologies provide definitions and standards that support implementation and interoperability across different systems. The initial NIST RBAC model and later versions are generic technologies, and the standards that specify definitions and establish a common RBAC foundation are based on infratechnologies. Infratechnologies have the characteristics of public goods; that is, they are commonly used by competitors and their customers (often in the form of standards). This creates free rider problems for companies that invest in their development. Further, infratechnologies typically derive from a different science and technology base than do the generic technologies and subsequent market applications (innovations) that they support. This fact leads to difficulties for firms and even entire industries with respect to capturing economies of scale and scope in the required R&D (Tassey, 2007).

NIST accelerated the introduction and acceptance of RBAC-enabled products in the marketplace, reducing uncertainty and setting the stage for software developers to assume leadership as the primary innovators in this space. NIST's contributions reduced the cost of early-phase (generic technology) R&D for private companies developing network security products based on RBAC. Interviews conducted during the 2002 study indicated that, in the absence of NIST, the development of generic RBAC technology would have been delayed, and the process by which that technology was developed would have been more inefficient. Thus, by demonstrating the technical feasibility of RBAC through its publications and conferences, NIST reduced development uncertainty and provided the technology base to accelerate the introduction of RBAC-enabled products into commercial access control systems and identity-aware software products.

The concept of using roles, either as a standalone mechanism or as part of a hybrid access control approach with ACLs and other mechanisms, is now widely known. However, uncertainty exists regarding the extent to which roles and their capabilities are actually employed. Organizations have large numbers of diverse applications and systems. Thus, integrating those systems using only one access control model remains unrealistic. What is known, however, is

that RBAC catalyzed a broad rethinking of how organizations' IT systems and processes could better align to the conduct of modern business practices. An ecosystem of access control software companies, role engineering and access control consultancies, and user-focused consortia have emerged in the last 20 years, and RBAC is a recurring topic of conversation at IT security and strategy events, including Burton Group's Catalyst Conferences and Gartner's Identity and Access Management Summit.

1.3 Study Objectives, Approach Overview, and Report Structure

The objectives of this economics study were to

- analyze the benefits and costs of RBAC, relative to other approaches, including ACLs, custom rule-based models, and mandatory access control;
- assess the actual rate of RBAC adoption from 1992 through 2009 and compare that rate with forecasts offered as part of the 2002 prospective analysis;
- conduct a comprehensive retrospective benefit-cost analysis and compare those results with net benefit projections estimated in the 2002 study;
- calculate measures of economic return on NIST's investment in RBAC;
- articulate key technology, business, and regulatory drivers affecting organizations' access control policies and procedures; and
- review the emergence of a value chain surrounding RBAC.

This report presents findings from 18 months of in-depth research into RBAC. We began by holding extensive discussions with subject-matter experts and IT managers to develop hypotheses about impact categories, review adoption drivers, and characterize adopting firms. A principal objective was to form the framework against which economic benefits might be quantified. Another was to engage each tier of the access control value chain—from developers through end users and auditors—to ensure that a complete taxonomy of economic benefit and cost categories was developed.

These discussions resulted in a survey that was fielded between July and September 2010, with responding organizations employing 2 million (4.5%) of 44.5 million people employed by organizations with more than 500 employees in 2010. In all, input from nearly 200 organizations in a host of industries provided the data underlying the analysis detailed in this report.

The report is organized as follows:

- Chapter 2, The Evolution of Role-Based Access Control, reviews key concepts and issues in access control and explains why RBAC was developed as an alternative to access control technologies that had been developed principally for the military and that were not effective for most nonmilitary organizations.

- Chapter 3, Advantages of Role-Based Access Control, discusses how RBAC can reduce the cost of provisioning IT permissions, the cost of maintaining access control policies, and new employee downtime for organizations that exhibit characteristics like large numbers of employees, high employee turnover, and well-defined and stable job positions. We also review how RBAC has the potential to generate substantial savings in governance, risk, and compliance activities.
- Chapter 4, NIST's Role in the RBAC Value Chain, explains the rationale underlying NIST's entry RBAC research in the early 1990s. We also review why NIST later stepped back from RBAC development once private-sector software developers took up further development of RBAC functionality, focusing instead on supporting RBAC-related standards.
- Chapter 5, Economic Analysis Methodology, explains that the economic benefits for RBAC-adopting organizations were measured relative to the use of rules and ACLs, net of ongoing operating costs and one-time adoption and implementation costs.
- Chapter 6, Analysis Results, reviews the calculation of $6,015 million in economic benefits (net of adoption costs) accruing from the use of roles to manage access permissions. This chapter also discusses current trends in RBAC as well as estimated RBAC adoption from 1994 through 2009.
- Chapter 7, Summary Results and Concluding Remarks, details the attribution of $1,107 million in economic benefits to NIST, which is equivalent to a net present value of $835 million (base year = 2000) when the social discount rate of 7% is applied and a benefit-to-cost ratio of 249.

2. THE EVOLUTION OF ROLE-BASED ACCESS CONTROL

This chapter provides background information on access control technologies and approaches, beginning with an introductory discussion of key concepts and issues in identity and access management (IAM).

2.1 Identity and Access Management: Key Concepts and Critical Issues

Information security requires an infrastructure that ensures people are who they say they are and provides users their appropriate level of access. Organizations must balance the benefits and costs of granting users IT permissions to arrive at the desired access control policy. They also must protect their IT resources from breaches of security, both accidental and intentional. In essence, access control policies specify who, and under what circumstances, has access to what.

An access control policy may be general and apply to all departments in an organization, such as a security-level clearance policy in the military, or it may be specific to the structure of a particular department, such as accounting. An organization's access control policy is a response to

- business drivers, such as lowering the cost of managing employees' permissions;
- security drivers, ensuring information security, integrity, and availability; and
- regulatory drivers, such as when enterprises seeking to comply with the Health Insurance Portability and Accountability Act (HIPAA) or the Sarbanes-Oxley Act of 2002 (often referred to as "SarbOx" or "SOX").

In organizations with few users or few resources to protect, maintaining an access control policy may be as straightforward as assigning access through an ACL—a list of users granted access.

For many organizations, especially medium and large ones, maintaining an access control policy requires a substantial dedication of resources because of the large number of users, objects, and systems. The more complex the IAM policies become, the more likely it is that they will contain errors from changes in regulations, implementation of new systems and policies, interactions among policies, or human error (Ni et al., 2009). It follows that technology that optimizes access control policies' effectiveness and efficiency offers substantial economic benefits.

2.1.1 Permissions, Operations, and Objects

Permissions, sometimes referred to as privileges or entitlements, specify what operations a user may perform on a specific object. Typical operations include read, write, delete, and execute, or complex transactions such as a money transfer. Typical objects are databases, applications, folders, and files.

Databases typically harbor information in tables. Users can create new tables, add new information to existing tables, or modify information that exists in the tables. Modern database applications allow for sophisticated access control policies to be used through their broad array of permissions. A user may have permission to read a table within a database containing sales information but may not be granted permission to modify any of the entries in that table.

Applications are the executable programs that individuals use. These can include common word processing and spreadsheet applications, as well as communication applications such as e-mail or Web conferencing. For many applications, there is only a single permission allowing a user to execute the application. As identity-aware applications have matured, however, more sophisticated access control policies can be implemented. Collaborative project applications allow team members to work together more effectively while keeping the underlying information secure.

Files and folders within operating systems also have their use regulated through access control decisions. Physical IT assets such as servers, routers, and printers further allow for the enforcement of an access control policy. As the number of identity-aware target systems increases, the demand for better tools to manage the permissions efficiently increases.

2.1.2 Authentication and Authorization

Access control is an important component of identity and access management (IAM). IAM refers to the spectrum of tools and processes that organizations use to manage the users of their IT and physical infrastructure, encompassing both the practice of managing users' identities and authorizations in a networked environment and the software and computing resources that authenticate identities and assess authorizations.

Authentication refers to determining whether users are who they say they are. Bank ATMs require the presence of both a bank card and the knowledge of a personal identification number to access bank accounts and perform transactions. For most organizations, the most common technique is to require a username and password pair to verify a user's identity. More advanced technologies are gaining popularity, such as biometric authentication, which uses retinal scans or fingerprints, and security tokens, which may change a portion of a password every 30 seconds and display that change to users via a fob or similar device.

Authorization refers to determining the permissions a user has and enforcing those permissions. In other words, authentication permits users access to a system by validating or verifying their identity. Authorization specifies what objects the user may access and what operations she may perform. Thus, access control is the authorization component of IAM.

2.1.3 User Life-Cycle Management and Provisioning

The implementation of an access control policy can be described through the lens of user life-cycle management, which is the series of steps involved in managing a user's identity and

permissions. The task of assigning, terminating, and modifying users' permissions is referred to collectively as provisioning.[1]

When a new user joins an organization, he must be given all of the permissions necessary to perform his job. Likewise, if a user changes positions or responsibilities, additional permissions must be provisioned and the permissions that are no longer appropriate for his job function should be removed. The process by which access permissions are removed from users is referred to as "deprovisioning." When a user leaves the organization all permissions must be terminated.

To understand what access control policy is in place, an organization must be able to review users' permissions. This involves not only ascertaining the permissions users currently have but also understanding what these permissions allow these users to do. To properly deprovision, an organization must know what permissions a user currently has and which of the permissions are no longer appropriate for the user's business function.[2] Acquiring this information requires time by IT administrators, human resources (HR), and management. Failure to deprovision will result in the enforcement of an undesired and unknown access control policy.

Until the past decade, most permissions were assigned to users using ACLs because flexible access control models were not available; an IT administrator usually enforced a desired access control policy entirely by adding and removing permissions or users from an ACL. Maintaining all of the user permissions within a central directory simplifies provisioning by assigning all of the permissions in one place and is an important component of IAM. However, this still requires that all user-permission assignments are created directly and that they are removed when they are no longer needed. But, in addition to the significant time cost of provisioning and deprovisioning, reviewing the access control permissions for a single user requires the administrator to review all ACLs. Performing these reviews regularly for all users becomes an extremely costly review process.

2.1.4 Overentitlement, Underentitlement, and Toxic Combinations of Permissions

An access control policy that strictly adheres to least privilege may be too costly to implement in practice. In this case, organizations must choose between implementing an access control policy that gives some users too many permissions ("overentitlement") or too few permissions ("underentitlement"):

---

[1] The term "provisioning" has its origin in the telecommunications industry and dates to the 1960s. It referred to preparing networks and systems to accommodate the addition of a new user. In the IT industry, the term refers to the assignment of system resources and permissions to new users.

[2] An access control system includes administrative, system, and review functions: 1) administrative functions allow for the assignment and removal of permissions from users, 2) system functions make and enforce access control decisions, and 3) review functions allow administrators to review the existing access control policy and potentially an auditable track of access to resources.

- An overentitled user presents a security risk. There is a greater chance that the user will have a toxic combination of permissions that allow violation of intended policy.
- An underentitled user presents both a business risk and security risk. If a user has too few permissions to do his job effectively, then the organization will lose productivity. An underentitled user will also seek to circumvent the access control system to complete his job, for example, by using another user's account to access the necessary information. This poses a security risk by not having an accurate documentation of "who accessed what."

If deprovisioning does not occur, it may not affect a user's productivity, but it results in the user maintaining unnecessary or inappropriate permissions. This phenomenon is referred to as permission drift and results in "overentitled" users. Overentitled users may possess what is referred to as a toxic combination of permissions, which would enable a user to break the law, violate rules of ethics, damage customers' trust, or even create the appearance of impropriety (Sinclair and Smith, 2008).

2.2 Access Control Models

Access control models are abstractions that incorporate the rules and parameters required to execute access control policies (Figure 2-1). Since multiple mechanisms can be constructed to support a particular access control policy, access control models provide a framework for policy implementation. Application of the model promotes consistent access control mechanisms across platforms, which lowers costs, increases security, and supports interoperability (Gallaher et al., 2002).

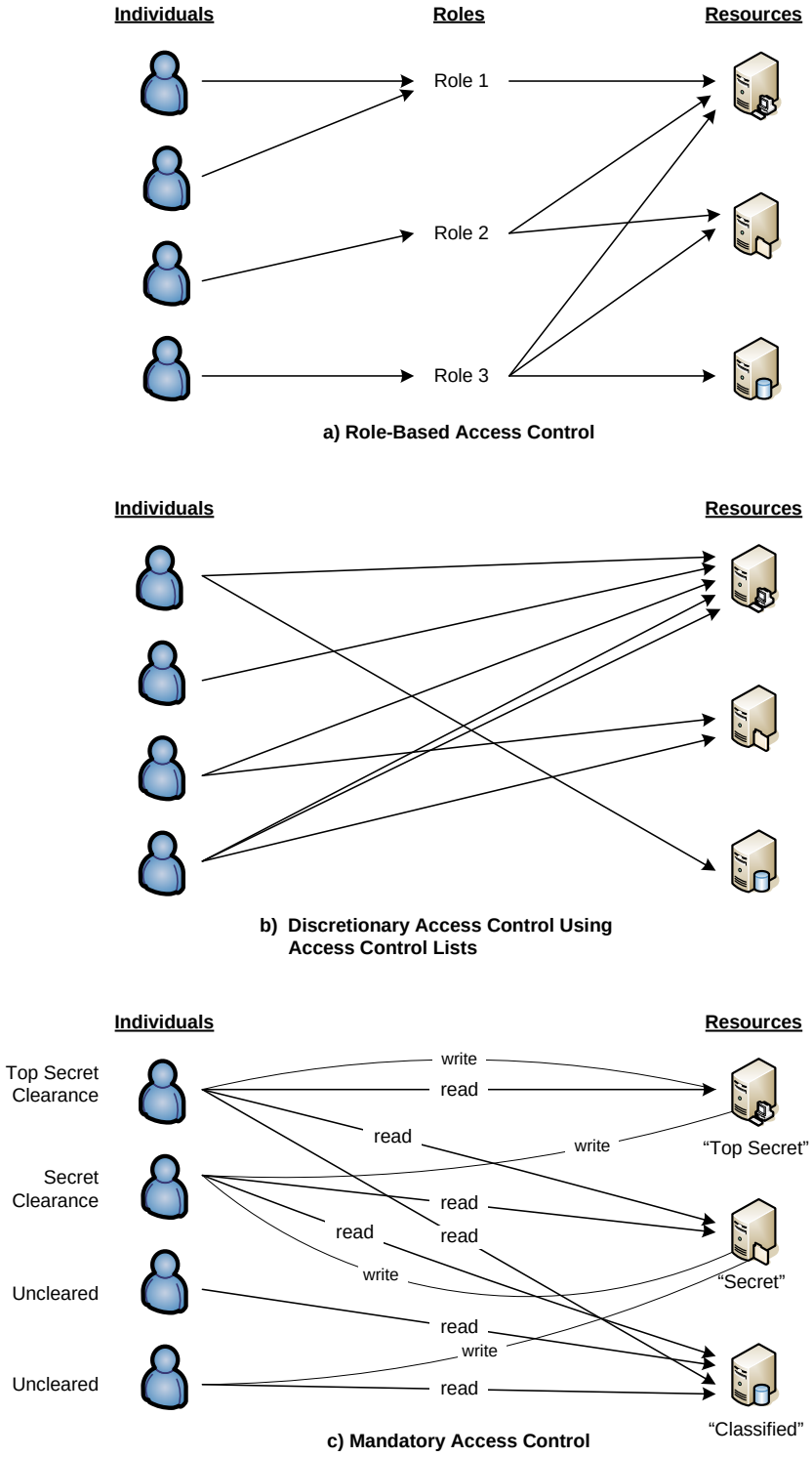
Early access control models were developed for defense-related applications and began to be formalized mathematically in the 1960s and 1970s. Two important models for the military—Discretionary Access Control (DAC) and Mandatory Access Control (MAC)—were specified in detail with the 1983 release of *Trusted Computer System Evaluation Criteria* (TCSEC), also referred to as the Orange Book. ACLs, MAC, and DAC largely dominated access control theory and practice until RBAC was introduced in the 1990s.

2.2.1 Access Control Lists and Capability Lists

As mentioned earlier, ACLs are the most prevalent and simple form of access control. An ACL is a list of users or groups of users and their permissions associated with a specific resource. Any user trying to access the resource will only be permitted to according to the parameters specified in the ACL.

Manually applied rules are often used in combination with ACLs, where ACLs are the repository of authorized users and the rule specifies what the users listed in a given ACL are permitted to perform. Before RBAC, rules and ACLs were the predominant method of managing access control. (Systems that can enforce arbitrary rules at run time are often called "rule based" or "attribute based.")

Figure 2-1. Alternative Access Control Methods



While ACLs are resource specific, capability lists are user specific. Capability lists are lists of resources and permissions associated with a specific user. Capability lists solve the problem of determining the resources a user has access to, but they make it difficult to determine what users have access to a specific resource.

It is possible to enforce a specified access control policy by assigning users to ACLs and many organizations rely on this approach, but maintaining ACLs to reflect the desired access control policy is labor intensive. A user may eventually receive his necessary permissions by request; however, requests to remove permissions are rarely made.

2.2.2 Groups

Many systems provide a means of placing users into one or more groups, with permissions attached to both a group and individual users within the group. In some cases, this approach can be nearly equivalent to the most basic form of RBAC (i.e., without hierarchies or constraints such as separation of duty), although the ability to attach permissions directly to users may lead to leaking privileges in unintended ways.

2.2.3 Discretionary Access Control

DAC is not a fixed set of rules to determine access, but rather a mechanism for how permissions are assigned to users. Generally speaking, the model dictates that the owner of a resource has the ability to grant (at her discretion) users access to the resource. Thus, because users can give away permissions, the access control policy enforced may deviate from the organization's desired access control policy. Administering access control using ACLs is one implementation of DAC.

2.2.4 Mandatory Access Control

MAC is a policy-specific, nondiscretionary access control model. MAC was developed to implement a multilevel security (MLS) access control policy, in which permissions are determined according to the user's clearance level (e.g., Classified, Secret, Top Secret). It is nondiscretionary, meaning that the rules governing access are not subject to change at the discretion of system administrators. Thus, the desired access control policy is always the access control policy enforced.

Although MAC is well suited for the military, most other organizations do not conform well to the MLS structure enforced with it. In fact, the diversity and complexity of commercial organizations require that a useful access control model be policy independent. To maintain enforcement of the desired access control policy, a useful model would need to be nondiscretionary. It is within this context that the formal model of RBAC was developed.

2.2.5 Attribute-Based Access Control

There is little consensus on what is meant by attribute-based access control (ABAC) (Kuhn et al., 2010); however, the basic concept is that each user and resource has a series of attributes that are known about them. Through a comparative assessment of situational data, such as time of day or persons logged on to the network, and known information about a user, such as title and location, the access control system can make near-instantaneous decisions about whether a user is appropriately authorized to perform an operation on an object. The data elements analyzed are referred to as attributes. The advantage of ABAC is that it leverages known information about users and contextual information, thereby avoiding role engineering (i.e., the process of designing a role structure). The disadvantages are that attributes may not be defined consistently, the access control policy becomes more dynamic than would be preferable for audit and attestation, and it requires specifying a large number of rules, making analysis difficult.

2.3 Role-Based Access Control

The RBAC model introduced the framework for using roles within access control. Recall from this report's introduction that rather than assigning permissions directly to users, under RBAC, permissions are assigned to roles engineered in software systems and users are assigned the roles necessary to do their jobs. Permissions can be grouped into roles based on location, business function, department, or other attributes of users, for example.

In 1975, Saltzer and Schroeder identified eight principles of design to enhance security within computer systems (Table 2-1). The RBAC model specifically enables the achievement of two of these principles, "least privilege" and "separation of privilege," and contributes to the principles of "economy of mechanism" and "psychological acceptability." The principle of least privilege states that users have only the permissions necessary to perform their job functions. Least privilege minimizes the impact of deliberate or accidental damage to a system, as well as limits the chance that a toxic combination of permissions exists. Strict adherence to least privilege, however, is difficult to implement in practice. RBAC provides the best framework to achieve least privilege within complex organizations.

The principle of separation of privilege, also referred to as SoD, is exemplified by requiring the correct authorization of two individuals prior to launching a weapon. Any task of a sensitive nature, from making a purchase to launching a missile, is made more secure when a single person is not able to execute all of the necessary tasks. The transformation of business processes from analog to digital has eliminated or obscured prior physical SoD controls. RBAC can be used to enforce SoD within digital systems by identifying toxic combinations of permissions and rendering them mutually exclusive. RBAC's use of roles as an abstraction of the connection between users and privileges simplifies management, contributing to economy of mechanism and making correct privilege assignment easier because roles reflect user jobs.

Table 2-1. Saltzer and Schroeder's Eight Principles of Secure Design for Computer Systems

	Principle	Meaning
1	Economy of mechanism	The system should be as simple as possible.
2	Fail-safe defaults	The default is denial of access.
3	Complete mediation	Every access decision must be checked.
4	Open design	The design must be open to review.
5	Separation of privilege	Sensitive tasks should not be completed by a single individual.
6	Least privilege	Users should not possess extraneous privileges.
7	Least common mechanism	The fewer the number of users sharing a mechanism, the less problematic a user damaging the mechanism will be.
8	Psychological acceptability	The security interface must be easy to use, or it will not be used correctly.

Source: Saltzer, J.H., and M.D. Schroeder. 1975. "The Protection of Information in Computer Systems." *Proceedings of the IEEE* 63(9):1278-1308.

RBAC is recognized for simplifying access control administration and improving visibility of both the access control policy and the organizational structure (Gallaher et al., 2002):

- When a user changes positions within an organization, provisioning is simplified by assigning the appropriate roles to the user rather than assigning all of the underlying permissions to the user.
- Deprovisioning is automated by removing the roles that no longer apply to the user's new position. If the organization upgrades a system, an IT administrator needs to only update the new permissions to the appropriate roles, and the permissions will be propagated to all relevant users via roles.
- Review of the access control policy is made easier because roles already may contain the user and permission information in a central location. Understanding the access control policy that is currently enforced within the organization is crucial to identify security threats and may aid in the attestation and auditing required by law.

In 2004, the American National Standard and International Committee for Information Technology Standards (ANSI/INCITS) approved an RBAC standard that combined features of the models introduced in Ferraiolo and Kuhn (1992) and Sandhu et al. (1996). The standard defined four levels of RBAC with their respective administrative, system, and review functions:

- core RBAC,
- hierarchical RBAC,
- static separation of duties (SSD) RBAC, and
- dynamic separation of duties (DSD) RBAC.

2.3.1 Core RBAC

Core RBAC delineates the basic elements and functions that are contained in every level of the RBAC standard. The basic elements are users, roles, and operations and objects that combine to form permissions. Core RBAC functions can be disaggregated into

- administrative functions, which include creating and deleting users and roles and creating and modifying user-to-role assignments and permission-to-role assignments;
- system functions, which include creating a user session that activates the user's roles and determining access decisions based on the user's roles;
- mandatory review functions, which include reviewing users assigned to a given role and roles assigned to a given user; and
- optional review functions, which include reviewing permissions assigned to a given role and permissions assigned to a given user.

2.3.2 Hierarchical RBAC

Hierarchical RBAC provides for the establishment of role hierarchies, with senior roles adopting all of the permissions within junior roles. This has the potential to simplify RBAC administration by streamlining the number of roles to which permissions and users are assigned. To realize these benefits, however, an organization must be structured hierarchically. Where this is not the case, hierarchical RBAC may add complexity that outweighs the benefits of simplified administration. Administrative functions within hierarchical RBAC include those within core RBAC as well as functions to establish inheritance relationships between junior and senior roles. System functions are the same as in core RBAC, with the addition of activating all roles junior to a user's roles. Review functions are the same as in core RBAC; however, these functions must take into account the hierarchy of roles when reviewing the access policy.

2.3.3 Static Separation of Duties RBAC

SSD RBAC allows for the creation of sets of mutually exclusive roles that, together, would allow users to possess a toxic combination of permissions (a set of permissions that would allow a single person to perform a critical operation—see Table 2-1). It is static because the SoD constraints are enforced at user-role assignment, rather than dynamically based on previous user actions. Administrative functions include all those associated with core RBAC, as well as creating, deleting, and modifying an SSD relation, as well as setting the cardinality of the SSD role set. The cardinality determines the number of users to whom the entire set of SSD roles could be assigned, thus violating SSD, but in a known and limited way. Since the SoD constraint is enforced at the user-role assignment stage, SSD RBAC system functions are the same as core RBAC. Additional review functions for SSD RBAC allow review of the current SSD relations, the set of roles within a particular SSD relation, and the cardinality of an SSD role set.

2.3.4 Dynamic Separation of Duties RBAC

DSD RBAC, as in SSD, allows for the creation of sets of mutually exclusive roles that, together, would allow users to possess a toxic combination of permissions. The difference is that users may be assigned to mutually exclusive roles; however, users will not be able to activate both roles simultaneously. For instance, a user may be able to request and approve purchases, but he would not be able to perform both duties on any purchase. Administrative functions include creating, deleting, and modifying a DSD relation, as well as setting the cardinality of the DSD role set. Additional system functions include enforcing the specified DSD constraints during a user session. Upon activating a user session, a user must not be assigned all authorized roles because some are mutually exclusive. Rather, the user will add active roles throughout the session, and the permission to add authorized roles will enforce DSD constraints. Review functions include reviewing established DSD relations, the set of roles within a particular DSD relation, and the cardinality of a DSD role set.

3. ADVANTAGES OF ROLE-BASED ACCESS CONTROL

This chapter catalogs RBAC's principal advantages and reviews common implementation practices. National cost-benefit estimates are presented later in the report; this section synthesizes anecdotal evidence elicited from our interviews with experts, government agencies, and companies. The five categories of benefits are

- more efficient access control policy maintenance and certification,
- more efficient provisioning by network and systems administrators,
- reduction in new employee downtime from more efficient provisioning,
- enhanced organizational productivity, and
- enhanced system security and integrity.

3.1 More Efficient Access Control Policy Maintenance and Certification in an Era of Increased Regulation of Internal Controls

RBAC facilitates and, relative to other approaches, reduces costs associated with four interrelated governance, risk, and compliance (GRC) activities through greater visibility of permissions assigned to users and easier verification of internal controls:

- access control policy maintenance,
- attestation of access control policies in place,
- certification of regulated information systems, and
- access control policy audits conducted by internal and external auditors.

Although information security is addressed in many regulations, the requirements mandated by HIPAA, the Graham-Leech-Bliley Act of 1999 (GLBA), and Sarbanes-Oxley are the most significant because they affect the information security activities of the entire health care and financial services industries, as well as publically listed companies (OCRP, 2003; Federal Trade Commission, 2002; SEC, 2008).[1] These acts explicitly dictate minimum standards for access control policies and information security.

To protect the confidentiality of both individuals and their personally identifiable information, recent federal laws have included provisions that dictate the type and the extent to which individuals' information can be shared both within an organization and with others. These laws require data managers to securely maintain and limit the distribution of data. To comply, companies are required to use access control policies that will safeguard data.

[1] The 2002 study discussed RBAC's relevance to HIPAA and GLBA; Sarbanes-Oxley was enacted following the release of that study and is new to the economic analysis.

3.1.1 Health Information Portability and Accountability Act

HIPAA seeks to protect individuals and their personally identifiable information by regulating the categories of information and extent to which it may be shared within an organization and with third parties. HIPAA is a health care reform initiative enacted in 1996 to add a dimension of portability to workers' health insurance as they transition between states of employment. HIPAA also contains privacy provisions that apply to health information created or maintained by health care providers who engage in certain electronic transactions, such as health plans, and health care clearinghouses.

To meet privacy compliance obligations, entities must maintain secure information systems that have the functionality to prevent the willful or unintentional disclosure of any individual's health records and or personal information to unauthorized parties. HIPAA regulates the use of protected health information and the instances in which it can be accessed under the privacy rule. The security rule sets implementation standards to ensure that electronic protected health information is accessed in accordance with the privacy rule.

Although HIPAA does not explicitly mention any given access control model in the final rule, its implementer, the Department of Health and Human Services (DHHS), specifically espouses RBAC as a security model to safeguard health data. In fact, in 2001, DHHS's Health Care Financing Administration (HCFA), now the Center for Medicare & Medicaid Services (CMS), referred queries about role-based access to NIST publications and the NIST Web site in its "General Questions" section about HIPAA. Responding to one question about role-based access, HCFA writes "please review Chapter 17—'Logical Access Control' of NIST SP 800-12, 'An Introduction to Computer Security: The NIST Handbook'" (HCFA, 2001).

3.1.2 American Recovery and Reinvestment Act

The American Recovery and Reinvestment Act (ARRA), passed in 2009, includes a provision in the Health Information Technology for Economic and Clinical Health (HITECH) Act expanding the HIPAA privacy and security requirements. This includes extending the entities covered by HIPAA to the business associates of covered entities, expanding the pool of organizations that must meet the HIPAA privacy and security requirements, and improving enforcement of HIPAA. The new provisions require health care organizations to report any breaches in the security of personal health information to patients whose information was compromised. Organizations must also maintain a breach log. IAM systems can aggregate authorizations and help develop logs under these new provisions.

3.1.3 Graham-Leech-Bliley Act of 1999

The GLBA eliminated the prohibition of retail and commercial banking, investment banking, and/or insurance activities within the same enterprise that dated from the Depression-era Glass-Steagall Act of 1933. Although the main objective was to increase competition in

previously tightly regulated markets, the provisions for protecting consumer information generated much interest (Ledig, 2000).

GLBA gave consumers the authority to block the exchange of any information concerning themselves or their accounts among or within companies except as concerns the maintenance of their accounts. The Act specifies the manner in which personal data can be exchanged among companies and among divisions of companies. It also lays out which information must be held in confidence and which can be distributed in aggregate form, if at all.

GLBA's Safeguards Rule requires financial institutions that hold personal consumer information to have a security plan in place to protect the information. The Federal Trade Commission, responsible for enforcing the Safeguards Rule, recommends that financial institutions consider "limiting access to customer information to employees who have a business reason to see it." This recommendation is best met using an RBAC-enabled IAM system.

3.1.4 Sarbanes-Oxley

Whereas HIPAA and GLBA apply confidentiality constraints on consumer information, Sarbanes-Oxley requires rigorous internal controls of the financial accounting of publicly held firms and their auditors. Rather than confidentiality of information, integrity of information is the prevailing aspect of Sarbanes-Oxley. Among other accountability and internal controls measures, this Act requires that public companies implement and report on internal controls in place to maintain the accuracy of financial reporting data. RBAC is considered a best practice in implementing the SoD and access monitoring required by law to attest to adequate internal controls.

As quoted in a 2005 article in *Network World*, "[w]ith Sarbanes-Oxley, the regulators want to know who was in what system, what they did, why they were there, whether they were authorized to be there, and how long they were there. You have to be able to answer those questions for almost everything. … From my perspective, without a role-based access control system, compliance is going to be a Herculean task" (Bednarz, 2005, p. 1). Sarbanes-Oxley was enacted in 2002.

3.1.5 Federal Information Security Management Act

The Federal Information Security Management Act (FISMA), passed as part of the E-Government Act in 2002, requires that all federal agencies develop and implement an information security program for all of their information and information systems, including those managed by government contractors. Information systems are placed into security categories of low, moderate, or high based on the level of adverse effect a lapse in information security would have. For each security category, NIST provides guidance for the appropriate security measures to implement, including aspects of the access control policy needed. RBAC is recommended as a security improvement (NIST, 2009).

3.1.6 Payment Card Industry Data Security Standard

Although the Payment Card Industry Data Security Standard (PCI DSS) is not mandated by regulation, all organizations that process cardholder information must adhere to the standards. Requirement 7 of the PCI DSS, which requires that cardholder data access be restricted by business need to know, specifically requires that privileges to access cardholder information are assigned using RBAC (PCI Security Standards Council, 2009).

3.1.7 Basel II

In 2004, the Basel Committee on Banking Supervision issued the International Convergence of Capital Measurement and Capital Standards: A Revised Framework, also known as Basel II. This document updated Basel I to include operational risk alongside credit risk as risks influencing capital requirements. Internal controls on information security are an important component of operational risk.

3.2 More Efficient Provisioning by Network and Systems Administrators

RBAC reduces the costs of administering and monitoring permissions relative to ACLs and other antecedent access control models. RBAC allows for greater automation, while adhering to the specified access control policy. Rather than manually assigning permissions whenever a new user is hired, an existing user changes positions, or new applications or IT systems are adopted, these changes are automated through role assignment.

Several issues must be weighed when granting access permissions. IT managers need to balance the

- complexity of the position being assigned privileges,
- complexity of the organization,
- security level required,
- data and application needs of the position, and
- organizational issues.

By assigning a predetermined role to the user, the labor expense of assigning permissions is significantly reduced, thus freeing resources for other tasks. Several attributes influence the magnitude of the expected cost decrease:

- The greater employee turnover or the number of people changing roles, the greater the cost savings of RBAC relative to other access control systems.
- Some firms or organizations are very dynamic, and user roles and permissions change quickly. In these environments, RBAC is more efficient in moving users in and out of static roles and changing the permissions of given roles than competing access control systems.
- RBAC reduces the provisioning decisions managers need to make. In alternative access control approaches, upper management is integrally involved in determining

individual privileges and authorizing access for each new employee. RBAC supports the automation of this process.

- RBAC is scalable, meaning that the model can work as well in large environments covering several offices and classes of users as it can in one-office environments. Roles matching job positions can be determined in a central office, but the actual assigning of roles to or changing of roles for new employees can occur at each branch office by an administrator. This concept, frequently referred to as "delegated administration," can be of particular benefit to organizations with several branches, subsidiaries, or contractor locations, such as health care plans, insurance companies, banks, and similar organizations.

3.3 Reduction in New Employee Downtime from More Efficient Provisioning

RBAC accelerates bringing "new" employees to full productivity. New employees are employees who have been recently hired or are existing employees placed in new positions within the organization. During this time period, these employees may only be marginally or partially productive because they are underentitled. These benefits greatly outweigh the benefits from greater efficiency in network and systems administrators' execution of provisioning tasks.

3.4 Enhanced System Security and Integrity

RBAC is designed to discourage the accumulation of a toxic combination of permissions by lowering the cost of administration and enabling the creation of SoD constraints. Using RBAC generally lowers both the probability and cost of access control breaches.

Costs due to inadequate access control policies can be extreme. Recall the earlier example in which a trader at Société Générale was able to circumvent their internal controls to execute fraudulent trades because of "entitlement creep." Back-office permissions allowing him to perpetrate the crime had never been removed from his account, costing the bank billions. Similarly, TJ Maxx had a phantom account on its system that stole credit card information (TJX, 2008). Adequate controls would have shown that the account did not belong to anyone, and it could have been stripped of its permissions and eliminated. National security-related examples include the WikiLeaks release of classified information in 2010. To prevent future leaks, the vice-chair of the Joint Chiefs of Staff recommended "moving to both identity- and role-based models so we know who's doing what and that they have the right credentials" (Reilly, 2010).

Costs resulting from inadequate controls exact a harsh penalty on the reputation of enterprises, as exhibited in market valuation. Perry and De Fontnouvelle (2005) show that losses based on internal errors are valued at approximately twice the actual financial loss, whereas losses caused by external factors are valued at the nominal (actual) rate.

Roles offer improved security and audit trails over alternative methods. RBAC reduces the impact from security violations in two ways. First, it decreases the likelihood that a security violation occurs, and second if a security violation occurs, RBAC can limit the damage from the

violation. Roles limit the possibility of internal security breaches from individuals who should not have access to the data and applications associated with each function. Because privileges are not assigned to each user manually, it is less likely that the security administrator will make an error and inadvertently grant a user access to information or applications to which she would otherwise be prohibited.

3.5 Enhanced Organizational Productivity

A major objective of RBAC has been to enhance security of information systems while not compromising system productivity. In fact, RBAC provides the underlying structure to streamline workflow management for organizations and user groups that are well-defined, such as that within a large grocery-store chain's retail operations or a call center, Because of the greater flexibility and breadth of network design associated with RBAC, the model can be adapted to mirror the organizational structure. This creates the potential for new and innovative ways of structuring the organization, altering the routing of information, or changing the organization's production processes (Kampman and Purdue, 2006).

Within workflow management systems, work is broken up into its components, some of which may need to be performed by different job functions. Using RBAC, the work can be funneled along and allow anyone of a particular role to execute the next portion of a task, avoiding bottlenecks associated with individuals in the process. These systems can enforce internal controls by not allowing a task to be considered "complete" until certain criteria are met.

RBAC creates a window into an enterprise that makes visible the impacts of business decisions and allows the organization to plan better for contingencies. For instance, if an enterprise is considering adopting a new application, it can use the access control system to discover precisely how many licenses would be required in adopting the application. Also, if a retail bank wanted to understand the impact of and develop a plan for closing a branch because of a natural disaster, they could analyze the duties of the employees working at the affected location by looking at their permissions and plan to transfer those duties among the remaining branches and corporate headquarters.

Organizations can benefit from the consistency in infrastructure across divisions or units within the same entity. The synergistic improvements that can occur within a company may have large impacts on employee productivity.

Finally, RBAC lowers the frictional cost of transition within and between enterprises. Businesses using RBAC can transition to new and better technologies and easily incorporate them into their access control policies through roles. No longer would a business be beholden to a legacy product because of costs associated with adapting the organization to a new system, since the system would be the same.

3.6 RBAC Implementation

Although RBAC can reduce provisioning costs by managing users and permissions with roles, it does not reduce the administration costs to zero. Implementing RBAC within an IAM system requires an up-front cost of creating the roles to be used, referred to as "role engineering" (Coyne and Davis, 2007). Once created, roles must be maintained to reflect changes to the access control policy and to the underlying information systems. This maintenance is referred to as "role life-cycle management."

The RBAC standard envisions all permission assignments and access control decisions to be mediated by roles. This would achieve "completeness" of the security system and ensure that no permissions granted outside of roles would be created that violate the desired access control policy. Managing all user permissions through roles, however, is not done in practice. Rather, a hybrid approach is taken, in which approximately some proportion of permissions are managed through roles, while the remaining proportion are managed through other means.

In interviews, we learned that even the most exhaustive role-engineering efforts will not incorporate every permission into a role. In fact, because so much can be done with RBAC projects, it is important to set concrete, achievable goals. Trying to "do it all" has resulted in project failure (Kampman, 2007).

After identifying RBAC as a valuable tool, a business will begin a role-engineering project. Defining the appropriate scope for the initial implementation of RBAC is a necessary and important step. Some RBAC projects in the early 2000s attempted to provision access across all target systems using RBAC. This proved to be too large of a project to succeed and resulted in some failures that dampened the enthusiasm for RBAC's potential. Today, role-engineering consultants advocate beginning the role-engineering project with the most important target systems to ensure early project success.

A successful role-engineering project will bring together the IdM stakeholders within the organization, primarily human resources, management, and IT administrators. These individuals possess the tacit knowledge of the organizational and technological infrastructure that role engineering makes explicit and transparent.

Having one group create and administer the security infrastructure represents a "combination of duties" security risk. In nondigital realms, HR and management staff determine who has access to what. The locksmiths did not decide who got a copy of the keys. Separating these duties in the digital realm requires an interface that HR and management staff can use. RBAC enables this visibility and returns security administration to those who are responsible for the consequences of an access control policy.

3.6.1 Permission Engineering

The first step in any role engineering is to organize and label the universe of IT permissions that are to be included in the access control policy. These IT permissions are the building blocks of roles. Labeling the IT permissions using terms that are easily understood by those at every level of the business will allow subject matter experts (SMEs), HR, and management to collaborate more effectively with IT professionals in the role-engineering process.

3.6.2 Top-Down Role Engineering

Top-down role engineering refers to developing roles by business and IT professionals to conform to a particular access control policy. For example, SMEs will determine the steps involved in a particular task, and IT professionals will determine the permissions necessary to execute those steps and assign them to a role. Although this process is labor intensive, it ensures that the roles created in the role-engineering process are understood and will be used appropriately.

3.6.3 Bottom-Up Role Engineering

Bottom-up role engineering refers to developing roles based on information used in the existing access control system, also referred to as "role mining." Role mining involves scouring the permissions contained within system ACLs and directories and using algorithms to group these permissions into roles. This process will succeed in creating roles that reflect the access control policy in place and improve provisioning of this access control policy. However, this process will not generate roles that are transparent and easily understood across the enterprise. In addition, if the access control policy in place is not the desired access control policy, then this process alone will simply turn an incorrect access control policy into an incorrect access control policy administered with roles.

3.6.4 Business Function and IT Roles

One important concept that has emerged is the necessity to successfully translate sets of permissions into roles that are easily understood across business units. This understanding is necessary to attest to what access control policy is actually in place. There may be a conflict here between parsimony of IT roles and the number of business functions (e.g., a Clerk and Loan Officer may need the same set of permissions; however, defining the role as Clerk or Loan Officer would make review of the access control policy not straightforward [That Clerk's not a Loan Officer!]).

3.6.5 Role Life-Cycle Management

Once created, roles will need to be continually maintained to ensure compliance with the desired access control policy. As with users, permission drift can occur in roles if unnecessary permissions are not removed over the life of the role. In this case, users may still accumulate a

toxic combination of permissions, however, now with the efficiency of roles. Proper maintenance of roles is necessary for correct adherence to a desired access control policy.

4. NIST'S ROLE IN THE RBAC VALUE CHAIN

NIST has been at the center of RBAC's development for nearly 20 years, having developed RBAC conceptual models and standards in response to industry's needs and later transitioning to a standards role for the generic technology as software companies assumed the mantle of extending its capabilities into a broad array of products.

As multiuser computer systems became more prevalent in the 1960s, researchers began exploring how access control could be established to promote information security. In 1983, the U.S. Department of Defense released the *Trusted Computer System Evaluation Criteria* (TCSEC), which presented access control models and technical specifications to protect confidential information, including MAC and DAC. Although these models were adopted outside of the military, MAC and DAC did not meet industry's access control needs in nondefense areas and were characterized by high maintenance costs. Unmet nonmilitary needs included a flexible access control system that gives users access to no more than they need to fulfill their duties (least privilege) and eases creating a separation of duties so that no one user can complete a sensitive task.

At that time, industry believed that a lack of standardization was hampering the development of appropriate access control products. A key to the success of such a system would be its ability to operate across a wide range of operating systems (Ferraiolo, Gilbert, and Lynch, 1992). Some systems included a rudimentary concept of roles, but there was no formal definition of RBAC, and role systems had few features beyond basic groups.

In response, NIST developed and published a comprehensive RBAC model in 1992, providing the first RBAC technical specifications and formal description (Ferraiolo and Kuhn, 1992), followed by an expanded model (Ferraiolo, Cugini, and Kuhn, 1995). These papers stimulated RBAC work by other researchers, including Nyanchama and Osborn (1994), and an influential paper by Sandhu et al. (1996). With R&D support through NIST program manager Tim Grance and a grant from NSA, NIST extended the understanding of RBAC by developing prototypes, incorporating different types of role relationships (Gavrila and Barkley, 1998; Barkley and Cincotta, 1998), and developing theoretical results (Kuhn, 1997; Kuhn, 1998).

NIST, with Ravi Sandhu, at the time with George Mason University, proposed a standard for RBAC in 2000 (Sandhu, Ferraiolo, and Kuhn, 2000) that integrated the models of Ferraiolo and Kuhn (1992) with that of Sandhu et al. (1996). This proposal was revised in 2001 (Ferraiolo et al., 2001) based on comments received, and NIST drafted the final standard proposal for the ANSI/INCITS RBAC standardization committee, led by Kuhn of NIST. ANSI/INCITS 359-2004, Role Based Access Control, was adopted in February 2004. Design decisions for the standard model are reviewed in Ferraiolo, Kuhn, and Sandhu (2007).

The proposals and adopted standard largely eliminated the uncertainty and confusion about RBAC's utility and definition; it has served as a foundation for software product

development, evaluation, and procurement specifications. NIST is also involved with developing standards for RBAC implementation and interoperability (INCITS CS1.1 Working Group). Lastly, revision of ANSI/INCITS 359-2004 is pending. NIST is leading development of changes to make RBAC more flexible for distributed environments (Kuhn, Coyne, and Weil, 2010).

This chapter, which is in part excerpted and updated from the 2002 study (Gallaher et al., 2002), reviews the barriers to RBAC development and implementation that existed in the early to mid-1990s, when the bulk of NIST's activity related to RBAC occurred.

4.1 Barriers to RBAC Technology Development and Integration into Software Products

Early barriers to developing and integrating RBAC models in commercial software products were symptomatic of RBAC's generic technology characteristics. These barriers included

- inadequate standards-oriented technical expertise from an independent organization,
- lack of a consistent definition for RBAC, and
- difficulty appropriating returns to investment due to the public-good nature of RBAC technology development.

The first two factors lead to uncertainty in the success and costs of RBAC research and development (R&D). The third factor leads to uncertainty in the company's ability to appropriate returns from its RBAC investments. All of these factors delay the availability of RBAC-enabled products. When appropriate, we discuss NIST's role in addressing these market failures.

4.1.1 Inadequate Standards-Oriented Technical Expertise

Although the concept of using roles was known to the programming community since the 1970s, there was a lack of understanding of RBAC's generic attributes, features, and capabilities. Because there was no generic RBAC conceptual model, there was little understanding of the programming requirements needed to operationalize RBAC meaningfully. This made software companies hesitant to commit to RBAC development; a level of uncertainty existed regarding the technical feasibility of developing successful RBAC-enabled products, what the development costs would be, and what the time frame for development would be. Thus, risk taking associated with developing commercial applications inhibited innovation, thereby resulting in low rates of investment in new RBAC-enabled software products.

NIST's project addressed such market failures by demonstrating the technical feasibility of roles through its programs. In addition, NIST's patents, papers, and the conferences have facilitated dissemination of the basic RBAC generic technology from which private companies have developed market applications.

4.1.2 Lack of Consistent Definition of RBAC

RBAC is a broad open-ended technology that ranges from very simple role structures to complicated hierarchies and constraints. As a result, the development of a single model was not appropriate. However, the lack of agreement on a set of fundamental concepts and underlying terminologies created a barrier to developing RBAC-enabled products.

As with the development of many new technologies, early models articulating RBAC features typically used different terminology to describe similar concepts and functionalities. The fact that the concept of roles simultaneously emerged from many different commercial and academic backgrounds contributed to the lack of consistent definitions and increased confusion.

Inconsistent definitions slowed RBAC's adoption. As a result, software developers had difficulty leveraging publicly available information, and consumers of RBAC products had difficulty evaluating and comparing different products. For example, RBAC was often confused with group access control mechanisms because of the superficial similarity between roles and groups, but group mechanisms have no support for separation of duty and little or none for hierarchies. The development of the NIST model and standard was the first successful attempt at presenting industry with a set of consensus RBAC concepts and terminology.

4.1.3 Difficulty for Private-Sector Developers to Appropriate Returns to Investment

RBAC models are generic technologies that can benefit a wide range of industries. It is a technology that will be integrated into a variety of products targeted at different market segments. As a result, it was difficult for the individual companies to fully appropriate the returns from their investments in generic RBAC technology because spillovers and imitation are likely to be high.

Like any technology platform, the generic RBAC conceptual model has the characteristics of a public good. Generic implies that once a base model has been developed it may be easily applied in numerous other commercial settings, including other companies appropriating the model for use in competing products.[1] RBAC is a generic technology for this very reason. The development of generic technologies is generally slow because they can be applied in numerous settings, industries, or firms. Additionally, appropriating the benefits to the innovating entity is difficult once the knowledge is generated and the technique is standardized.

[1] RBAC is a conceptual model for developing access control systems (i.e., it is a generic technology as opposed to an infratechnology, which is the primary output of NIST laboratory research). Infratechnologies are technical tools, including scientific and engineering data, measurement and test methods, and practices and techniques, that are widely used in industry (Tassey, 1997, 2007). The RBAC model itself is not an infratechnology because its main effect is to provide a technology platform (i.e., a generic technology) rather than leverage the efficiency of R&D, production, or market transactions.

Generic technologies have characteristics of public goods in that they exhibit nonrivalry and nonexcludability.[2] RBAC is nonrival because one firm's use of RBAC does not directly affect another firm's use. RBAC is also nonexcludable because one firm cannot prevent another firm from using the fundamental concepts of roles as the generic technology is advanced. Public goods are typically underprovided by private markets compared to their socially optimal levels of provision (Stiglitz, 1988).

Because of the appropriability issues, it is generally accepted that public-sector research organizations should fund research in generic technologies to the point where market applications become profitable for the private sector (i.e., where the risk-adjusted expected rate of return to investment in RBAC products exceeds the companies' internal rate of return criteria) (Scott, 1999).

NIST's involvement mitigates market appropriation issues by providing the research foundation to which all parties have access. Firms are then able to produce and market products that build on NIST's research and therefore incur only the incremental R&D costs for orienting the RBAC applications needs of their current and prospective products toward their customer base. This makes investment in RBAC-enabled products more attractive for the private sector and accelerates the availability of commercial RBAC-enabled products.

A second advantage of NIST's approach is the limitation of users being locked into a specific product or firm. When the generic technology is publicly available, software products from competing companies are more likely to be interoperable and work together in integrated systems. This increases competition and lowers barriers to entry in the access control market.

4.2 Barriers to Implementation of RBAC-Enabled Products

The second category of barriers to developing and adopting RBAC is implementation barriers that affect end-user purchase decisions and the organization's decision of whether to implement a role-based access policy.

In an ideal scenario, an organization will establish and design operations processes and then create an infrastructure that would execute those processes, providing to each member only the tools needed to perform his function (Byrnes, 1997). Information systems would be designed and built to support the roles that correspond to these processes. Each role would be assigned a series of permissions defined by their position and function within the organization. Ideally, the system would be clearly defined and agile, making the addition of new applications, roles, and employees as efficient as possible.

[2] Public goods, unlike private goods, are characterized by consumption nonrivalry and by high costs of exclusion. Rationing of such goods is undesirable because the consumption of a public good does not impose costs on society since it does not reduce the amount of the good available to others. Further, the costs of excluding those who do not pay for the infratechnologies are likely to be high because they are typically embodied in products and processes (techniques), rather than in products that can be sold.

However, the ideal scenario rarely occurs. Business processes and employee positions, both formal and informal, are preexisting and entrenched, impeding turn-key implementation of new systems and management philosophies. Because RBAC requires roles to be established within the workplace, organizations implementing a role-based system may need to complement their information-access policies with their general administration policies. Subsequent realigning of workflow and positions, to whatever extent necessary, may be very expensive, difficult, and time consuming.

One software developer noted that "RBAC [is] a tool that supports a correctly defined [administrative] policy….The structure and support model of the organization, as defined by that policy, will determine the cost savings, if any, should RBAC be implemented. Actually, RBAC will cost an organization more in the long run if the policy for that organization is not realistic in terms of operational requirements for RBAC or fails to even define RBAC and its use throughout the organization."

4.2.1 Role Engineering

As described in Chapter 3, the process of defining and implementing roles is known as "role engineering." Role engineering can be a contentious and time-consuming process, but it is integral to RBAC's success.[3] One developer said a customer's rollout of RBAC hit a large number of glitches precisely because "the overriding problem can be traced back to a lack of RBAC support in the organization's administration policy."

Role engineering entails defining the roles that will determine which employees have access to which data and to which applications, as well as roles' relationships to one another, role hierarchy, and role constraints. As this process progresses, implementers may see benefits in rethinking how work is allocated and completed within the organization. The INCITS CS1.1 Working Group aims to offer guidance on RBAC implementation.

Role-engineering expense has decreased over time because of the development of new software tools and increased familiarity with the process of defining and assigning roles. Several companies have developed or are in the process of developing software tools that help automatically define roles using existing patterns of access permissions gleaned from user databases. These tools reduce the labor expense of manually defining and creating all roles. Furthermore, as companies and consultants become familiar with the implementation process, a learning curve effect has emerged. However, the extent of these two developments' impact on role engineering is not clear. The relative ease or difficulty of the role definition process depends

[3] NIST developed an initial set of tools to assist end users in role engineering. The tools included RGP-Admin, a tool for managing role/permission relationships, and AccesMgr, a graphical user interface for managing ACLs for Windows NT files. Through the development of these tools, NIST lowered the cost of, and hence the barrier to, adopting and implementing RBAC-enabled systems. However, as expected, these tools have been superseded by private-sector product and service offerings.

on an entity's organizational and administrative structure—an attribute that varies widely among firms.

4.2.2 Migration Costs

Any time a new information system is installed, an organization accrues costs. This is especially true if the decision is to implement a new access control system. The costs of migrating to a role-based system are four fold: salaries and consultants' fees, software purchases and licensing agreements, computing resources and infrastructure, and customization costs. These costs may differ depending on the scope of the package being installed, the size of the firm or the number of licenses, and the migration complexity.

One of the largest cost components of installing an RBAC system is the salaries and benefits of the team tasked with its implementation. Tasks include not only the implementation and migration of the software system purchased, but also the staff training, software package selection, and the customization process. In addition to staff labor expenses, consultants may be hired to either implement the systems migration completely or to offer their expertise on some component therein. Outside consultants may also be hired to customize a prepackaged system or help with role definition.

In addition to purchasing the software itself, an organization may invest in software support services and new systems infrastructure. The software agreement may involve a sliding fee scale based on the number of licenses purchased and a software maintenance agreement. Depending on the package's system requirements, buyers may need to build or enhance their systems' infrastructure. The expense of buying, installing, and maintaining computing resources can be high. Costs may rise further if network resources must be maintained solely or partly to help migrate from one system to another.

4.2.3 Systems Structure and Interoperability

As new systems are installed, administrators may have to rectify years of inefficiencies, such as informal access grants, disorganized systems, and different organization structures among divisions. The move toward disciplined centralized systems often means realigning these systems and creating a more cohesive, formal systems structure. Because of the time and cost involved, it is likely that a large organization will adopt RBAC at an incremental pace. By spreading out implementation over a period of time or only when new applications or systems come online, companies avoid the risk-prone full rollout.

Security features need to be effective across sectors of the firm or organization without being overly intrusive to the user. This trait is referred to as interoperability. Interoperability is the ability to communicate and transfer data or information across different activities and platforms. For example, an access control system that displays perfect interoperability would be able to communicate with the security and administrative network across an entire firm without any disruptions or complications. Without a framework or architecture for addressing

interoperability problem, firms may be unable to implement RBAC and benefit from the reduced administrative costs and improved security.

4.2.4 Product Acceptance and Comparison

When making purchasing decisions, buyers of software products gather information about the various potential products and then make a decision based on the comparison of characteristics across products. These comparisons could include cost, quality, reliability, and capacity. For this process to be effective, consumers must have an understanding of what they are getting from a product, and producers must be able to prove that they are delivering what the consumer wants.

Prior to NIST's involvement, no commonly agreed-upon definition of RBAC existed. For example, some systems used the term "role" as a synonym for groups, and some had ad hoc implementations with a few hard-coded roles such as "manager" or "teller." Without a definition, firms that were interested in either upgrading their existing access control system or purchasing new access control systems had difficulty obtaining generic RBAC solutions and may have been unable to compare attributes across commercial products using roles.

Without a set of metrics that consumers are willing to accept as standards for a particular piece of technology, software firms are unable to prove that their product is reliable in addressing security issues and effective at reducing administrative costs. The entire industry was lacking a yardstick or common definition. If producers and consumers cannot agree on the product they are selling, market transactions are unlikely to happen or, at best, they take place more slowly and at higher cost—thereby reducing the rate of market penetration of the new technology. A study by NIST (Ferraiolo, Gilbert, and Lynch, 1992) found that part of the reason why commercially oriented approaches such as roles had not been implemented was the lack of a "stamp of approval" from a third party. Ferraiolo, Cugini, and Kuhn (1995) make this clear by stating "The lack of definition makes it difficult for consumers to compare products and for vendors to get credit for the effectiveness of their products in addressing known security problems."

NIST's work at defining RBAC has addressed this failure by engaging in efforts that generated a common yardstick that all software developers can use. Specific projects included surveys of security needs and the development of a formal RBAC model to demonstrate its effectiveness and reliability. A standardized RBAC model of this nature constitutes an infratechnology that has attributes of a public good in that it has the effect of lowering R&D costs and facilitating market transactions (Kampman, 2007). For example, developers and buyers can decide if they want to supply/purchase advanced features such as separation of duty support, or if basic RBAC with hierarchies is sufficient.

4.3 NIST's RBAC Activities

The papers NIST has published and the patents it has received have provided the technology base for many of the commercial products being introduced by software vendors (see Table 4-1). NIST has presented its work at a number of professional conferences geared toward senior scientists in software R&D and has cofounded the Association for Computing Machinery (ACM) Symposium on Access Control Models and Technologies (SACMAT), formerly the ACM workshops on RBAC.

Table 4-1. Overview of NIST's RBAC Activities

Category	Activities	Citation Count
Standards development	American National Standard/International Committee for Information Technology Standards (ANSI/INCITS), 359-2004. Based on "The NIST Model for Role-Based Access Control: Towards a Unified Standard" (Sandhu, Ferraiolo, and Kuhn, 2000)	
	INCITS CS1.1 Working Group, Towards a RBAC Implementation Standard	
	OASIS XACML Committee, RBAC Web Services Standard	
Patents	Implementation of Role-based Access Control in Multi-level Secure Systems (Kuhn). U.S. Patent #6,023,765	74
	Workflow Management Employing Role-Based Access Control (Barkley). U.S. Patent #6,088,679	121
	A Method for Visualizing and Managing Role-Based Policies on Identity-Based Systems (Ferraiolo and Gavrila) (pending)	
	Implementation of Role/Group Permission Association Using Object Access Type (Barkley and Cincotta, 2001). U.S. Patent #6,202,066	117
Selected papers	D. Ferraiolo, R. Sandhu, S. Gavrila, R. Kuhn, R. Chandramouli. "Proposed NIST Standard for Role Based Access Control."*ACM Trans. Inf. and System Security (TISSEC)*, 4(3), 2001	2,850
	"Role-based Access Control" (Ferraiolo, Kuhn, 1992), *Proc.15th Natl Computer Security Conf.*	2,831
	R. Sandhu, D. Ferraiolo, R. Kuhn. "The NIST Model for Role Based Access Control: Towards a Unified Standard." *Proceedings, 5th ACM Workshop on Role Based Access Control,* July 26-27, 2000, Berlin, pp.47-63	553
	"Role-based Access Control: Features and Motivations" (Ferraiolo, Cugini, and Kuhn, 1995), *Proc. Computer Security Applications Conference*	550
	"Mutual Exclusion of Roles as a Means of Implementing Separation of Duty in Role-Based Access Control Systems" (Kuhn, 1997), *2nd ACM Workshop on Role-Based Access Control*	147
	"Role-based Access Control for the World Wide Web" (Barkley, Cincotta, Ferraiolo, Gavrila, and Kuhn, 1997). *Proc., 20th National Computer Security Conference*	103
	Role-based Access Control (Ferraiolo, Kuhn, and Chandramouli, 2003, revised 2007)	86
	"Role-based Access Control Features in Commercial Database Management Systems" (Chandramouli and Sandhu, 1998), *21st National Information Security Conference*	67
	"Implementing Role-based Access Control Using Object Technology" (Barkley, 1995). *First ACM Workshop on Role-Based Access Control*	59

(continued)

Table 4-1. Overview of NIST's RBAC Activities (continued)

Category	Activities	Citation Count
	"Specifying and Managing Role-Based Access Control within a Corporate Intranet" (Ferraiolo and Barkley, 1997). *Second ACM Workshop on Role-Based Access Control*	41
	"Role-Based Access Control for the Web" (Barkley, Kuhn, Rosenthal, Skall, and Cincotta), *CALS Expo Intl. & 21st Century Commerce 1998: Global Business Solutions for the New Millennium*	18
Web tools and software	RBAC for UNIX/POSIX/LINUX RBAC for Windows NT	
	RGP-Admin	
	AccesMgr	
Industry outreach efforts	ACM Symposium on Access Control Models and Technologies (SACMAT), formerly the Association for Computing Machinery (ACM) workshops on RBAC	
	RBAC for Synergy	
	RBAC Small Business Innovation Research (RBAC SBIR)	
	Role Control Center (RCC)	
	RBAC for the World Wide Web (RBAC/Web)	
	Computer Security Resource Center RBAC Web Site	

Note: Citation counts from U.S. Patent and Trademark Office and Google Scholar (as of 11/9/2010).

NIST researchers, with Ravi Sandhu of George Mason University, proposed a standard for RBAC to codify the RBAC model (Sandhu, Ferraiolo, and Kuhn, 2000). In 2004, ANSI/INCITS adopted the industry consensus standard for RBAC, INCITS 359-2004, based on the NIST RBAC model. This voluntary standard allows customers to ensure that the RBAC products they adopt will have the components mandated in the RBAC standard. Currently, the INCITS Cyber Security RBAC task group (CS1.1) is working on an RBAC Implementation and Interoperability Standard (RIIS) to provide guidance for developers on conforming to the INCITS 359 standard, allow customers to make better comparisons of RBAC products, and support the interoperation of RBAC implementations (Coyne and Weil, 2008).

NIST supplemented its standardization activities, technology leadership, and technical community coordination function with tools for RBAC implementation. These tools were more critical during the first years of RBAC adoption but remain important contributions to the technology infrastructure supporting RBAC:

- implementation of RBAC on the NSA Synergy secure operating system;
- tools for implementing RBAC for the Web, such as RGP-Admin, a tool for managing role/permission relationships (Barkley et al., 1997);
- AccesMgr, a graphical user interface for managing ACLs for Windows NT files;
- demonstrations of RBAC for the Web for corporate intranets (Ferraiolo, Barkley, and Kuhn, 1999), the health care industry (Barkley, 1995);
- RBAC software and reference code; and

- Role Control Center as a reference implementation and a demonstration platform for the viability of advanced RBAC concepts.

4.4 The RBAC Value Chain

In the 18 years since NIST first published the core RBAC model, economic activity surrounding RBAC development, implementation, and use has become a complex interplay of economic agents (Figure 4-1). Accepting that organizations may add value and play roles at different stages of the value chain,[4] it is possible to generalize and segment the value chain into four broad groups:

- academic and standards community groups,
- enterprise software developers,
- systems integrators and consultants, and
- end users.

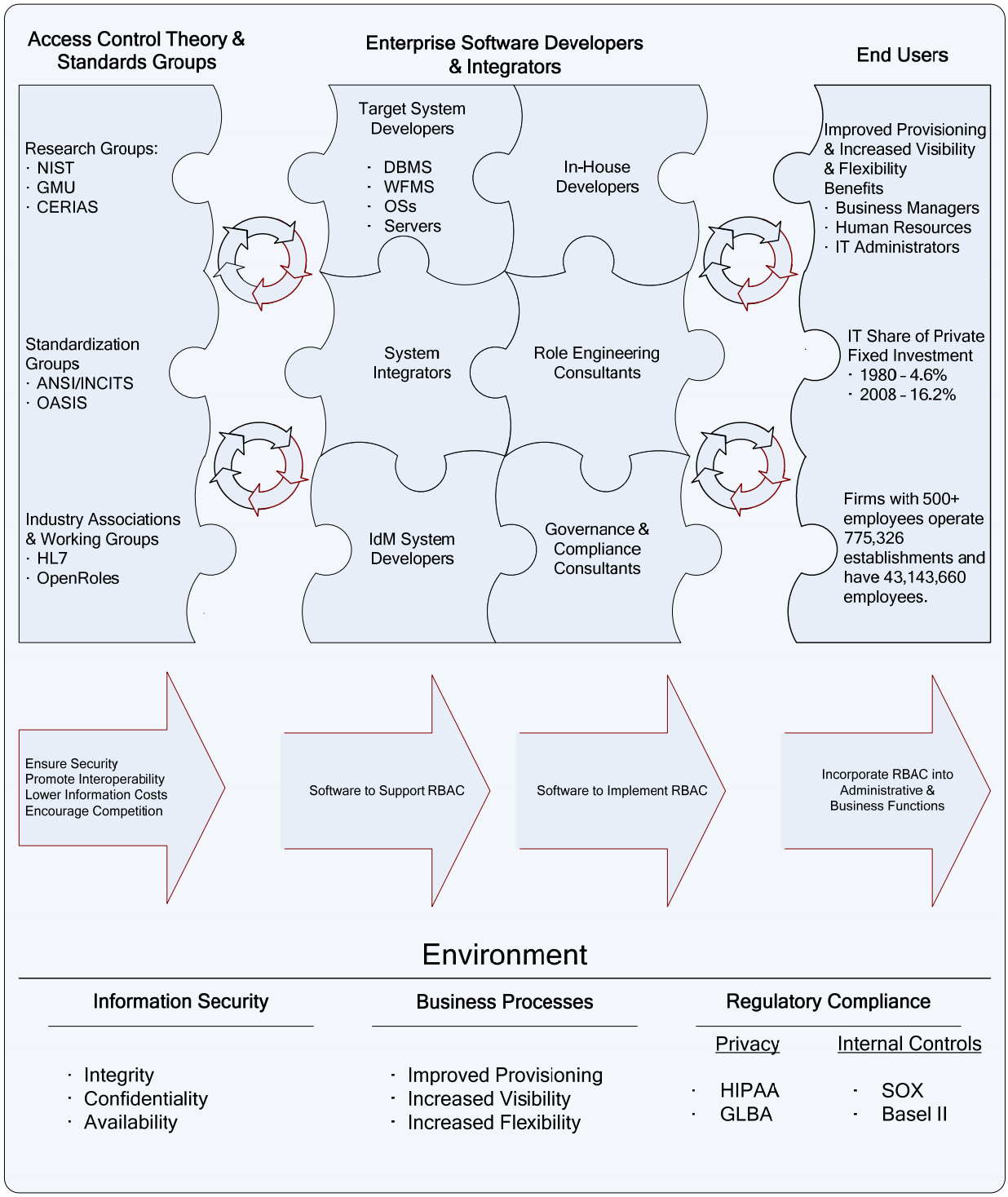
4.4.1 Academic and Standards Community Groups

Many groups have contributed, and continue to contribute, to the field of access control. Academic, government, and industry researchers develop and discuss cutting-edge research, such as models for distributed administration of RBAC and novel role-mining algorithms. Standardization groups bring together experts to codify these nascent, beneficial security technologies to support their adoption and interoperability with existing systems. Industry associations and working groups seek to tailor the technologies to achieve goals specific to their interests, but also may lead to more codified standards.

Since Ferraiolo and Kuhn of NIST introduced RBAC in 1992, the research community has evaluated and built on the concepts within RBAC. Much of this research has been presented at SACMAT sponsored by ACM and the ACM Special Interest Group on Security, Audit, and Control (SIGSAC). First held in 1995 as the ACM Workshop on Role-Based Access Control, 14 symposia have been hosted with presenters from government, industry, and academia. In addition to this research forum, many universities have research centers devoted to information security that continue to conduct research on RBAC, including George Mason University, the Institute for Cyber Security at University of Texas San Antonio, and the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University.

[4] Information security is such a critical issue that the development of models, implementation approaches, and software systems does not follow the traditional supplier-consumer paradigm. Software code is largely intangible intellectual property without capital expenditure barriers, and organizations will participate in its development if they perceive that the benefits of participating exceed costs. The value chain is not as discrete as that of the automotive industry. For instance, companies like Oracle and Sybase not only develop IdM systems, but they also have consulting arms that implement and customize their software and intellectual property for their customers.

Figure 4-1. RBAC Value Chain



To improve the effectiveness of RBAC and support its adoption by industry, many groups have collaborated to develop standards for RBAC. These standards accomplish many objectives, including

- providing customers and suppliers with a common understanding of what RBAC is to engage in the marketplace;
- improving the interoperability of heterogeneous systems by providing a common language and operation; and
- increasing competition in the marketplace by preventing monopoly control over customers through exclusive proprietary systems.

In addition to NIST's RBAC standards work, the Organization for the Advancement of Structured Information Standards (OASIS) has contributed standards to support the interoperability of IAM tools across heterogeneous target systems, such as the Security Assertion Markup Language (SAML) for authentication across target systems and the eXtensible Access Control Markup Language (XACML) for access control across target systems. OASIS has published a profile for implementing RBAC with XACML. Although XACML standardizes a syntax for heterogeneous target systems to communicate access control decisions, it does not specify the vocabulary necessary for the target systems to communicate successfully (Anderson, 2004).

In 2008, the Open Role Exchange was begun as an industry-led initiative to develop a standard operational context for heterogeneous identity-aware systems, each potentially with its own specified role model, to exchange information successfully as specified in the access control policy (Rolls, 2008). This initiative is endeavoring to build off of the existing standards to provide organizations with examples and tools to streamline the implementation of RBAC across a distributed and complex organization.

Health Level Seven (HL7) is an ANSI-accredited organization working to develop standards for exchanging clinical and administrative data. As part of this effort, HL7 began a role-engineering effort to define standardized permissions and constraints for the health care industry. This process will allow organizations to share medical information successfully in a transparent and HIPAA-compatible way.

4.4.2 Enterprise Software Developers, Systems Integrators, and Consultants

Many IT professionals contribute to and use RBAC in their professional roles:

- target system developers, who incorporate access control enforcement into the target systems;
- IdM system developers, who create the suite of tools for end users to manage users' identities and permissions across heterogeneous systems;
- in-house developers, who design custom software for the end user;

- system integrators, who integrate heterogeneous systems for the end user;
- role-engineering consultants, who provide technical expertise during the role-engineering phase of RBAC implementation; and
- governance and compliance consultants, who help end users leverage RBAC to develop the processes of review and attestation necessary for regulatory compliance.

Companies within the above categories fall primarily under the North American Industry Classification System (NAICS) categories Computer Systems Design and Related Services (NAICS 5415) and Software Publishers (NAICS 5112). In 2002, these two sectors generated $327.6 billion ($2008) in sales by U.S. establishments, with the most sales within the computer system design, development, and integration services product category ($62.9 billion) (see Table 4-2). There is substantial interplay within these groups of IT professionals. Many target system and IdM system implementations involve a back and forth between the developers and in-house IT staff to ensure that the software performs to the end users' specifications.

Although there continue to be many niche players, the software market is dominated by a select few dominant companies. In 2007, according to IDC, the top 5 software companies by revenues held 38% of the total market share, and the top 15 accounted for 50% of the total market share (Bokhari, 2009). Because most major software companies house a combination of software and services, there is an overlap of the above categories within companies. For instance, the Oracle 11g database is a sophisticated target system that allows for an application-specific access control policy to be administered using RBAC. In addition, Oracle Identity Management is an IdM suite that includes Oracle Role Manager, which allows multiple heterogeneous target systems to be managed centrally (see Table 4-3).

4.4.3 End Users

Although IT is used in every major industry, certain industries rely more heavily on IT than others. In 2007, the finance and insurance industry spent $15.6 billion on capitalized software expenditures, while the forestry, fishing, and agricultural services industry invested only $29 million (Table 4-4).

The network architecture within an organization consists primarily of workstations, servers, routers, and physical assets:

- Workstations are users' computers that allow them to connect to the network.
- Servers are the dedicated hardware that house the networked software and data for the organizations. Many types of designated servers are linked together in a corporate network, such as e-mail, database, Web, application, and operating system servers.
- Routers channel and control the traffic of information across the network.
- Physical assets, such as printers, allow authorized users to manifest digital information in the physical world.

Table 4-2. Software and Systems Integration Sales, by Product Lines, 2007

Product Code	Product Description	Computer Systems Design and Related Services (NAICS 5415)		Software Publishers (NAICS 5112)	
		Industry Sales ($ thousands)	% of Total Industry Sales	Industry Sales ($ thousands)	% of Total Industry Sales
31920	Electronic & precision equipment repair	$84,945	<1%		
32730	Temporary staffing services	$2,395,194	1%		
34880	System software publishing	$107,047	<1%	$54,142,577	40%
34890	Application software publishing	$612,014	<1%	$46,625,954	34%
34910	Information technology (IT) technical consulting services	$11,713,165	5%	$2,474,853	2%
34930	Application service provisioning	$1,719,757	1%	$1,570,063	1%
34940	Business process management services	$2,880,154	1%	$551,253	<1%
35620	Licensing of rights to reproduce & distribute computer software			$12,868,071	10%
36010	Internet access services	$108,813	<1%		
36120	Website hosting services	$734,474	<1%		
36140	Data storage services	$435,369	<1%		
36150	Data management services	$1,191,454	<1%		
37410	Custom computer application design & development services	$63,142,395	26%	$2,855,708	2%
37420	Network design & development services	$8,587,761	4%		
37430	Computer systems design, development, & integration services	$88,680,466	36%		
37500	Video & audio streaming services	$10,259,800	4%		
37510	IT infrastructure (computer) & network management services	$14,693,800	6%		
37520	Information technology (IT) technical support services	$24,787,634	10%	$7,126,244	5%
37570	Licensing right to reproduce/distribute computer software protected by copyright	$286,621	<1%		
37600	Rental & leasing of computer hardware	$100,465	<1%		
37610	Information technology (IT) related training services	$925,871	<1%	$720,739	1%
37630	Data analysis services	$438,131	<1%		
39280	Engineering services	$1,108,523	<1%		
39600	Resale of merchandise	$5,153,868	2%	$2,904,268	2%
30000	**Total Industry Sales**	**$244,389,132**	**100%**	**$135,400,841**	**100%**

Sources: U.S. Census Bureau; generated by RTI International; using American FactFinder; "Sector 54: Professional, Scientific, and Technical Services: Subject Series: Product Lines by Kind of Business for the United States: 2007." and "Sector 51: Information: Subject Series: Product Lines by Kind of Business for the United States: 2007" <http://factfinder.census.gov>; (December 6, 2010).

Table 4-3. Top Packaged Software Suppliers Globally, 2009

Rank	Company	Revenues ($ millions)	Market Share (%)	Example IAM System	Example Target System
1	Microsoft	48,112	17.67	Authorization Manager	Microsoft Exchange Server
2	IBM	23,622	8.68	Tivoli Provisioning Manager	WebSphere InterChange Server
3	Oracle Corp	19,973	7.34	Oracle Role Manager	Oracle Database 11g
4	SAP AG	11,295	4.15	NetWeaver Identity Management	SAP Enterprise Portal
5	Symantec	5,639	2.07	Altiris Client Management Suite	Enterprise Vault
6	HP	4,384	1.61	ProtectTools Role Based Access	HP-UX Operating System
7	CA	3,985	1.46	Role & Compliance Manager	AutoSys Workload Automation
8	EMC	3,825	1.41	RSA Access Manager	Celerra Network Server
9	Adobe	3,209	1.18	LiveCycle Rights Management ES	Cold Fusion
10	Fujitsu	2,637	0.97	Interstage Content Integrator	Glovia ERP Security Manager
11	Siemens	2,368	0.87	DirX Access	Teamcenter SRM
12	Intuit	2,150	0.79	NA	QuickBase
13	SAS	2,140	0.79	NA	SAS Enterprise BI Server
14	VMware Inc.	1,873	0.69	NA	vSphere
15	BMC	1,795	0.66	BMC Identity Management Suite	BMC BladeLogic Server Automation Suite

Source: Bokhari, Z. 2009. Standard & Poor's Industry Surveys, Computers: Software and company web sites.

Table 4-4. Expenditures on Capitalized Information and Communications Technology, by Industry, 2008

Industry	NAICS	Total ICT Equipment Capitalized Expenditure ($ millions)	Percentage of Total Industry Capital Expenditures	Software Capitalized Expenditure ($ millions)	Percentage of Total Industry Capital Expenditures
Forestry, fishing, and agricultural services	113–115	$60	2.79%	$29	1.35%
Mining	21	$1,343	1.10%	$520	0.43%
Utilities	22	$2,548	3.05%	$1,484	1.77%
Construction	23	$1,748	4.76%	$426	1.16%
Manufacturing	31–33	$18,547	9.42%	$10,469	5.32%
Durable goods industries	321, 327, 33	$10,922	10.11%	$5,821	5.39%
Nondurable goods industries	31, 322–326	$7,625	8.57%	$4,648	5.22%
Wholesale trade	42	$6,119	19.27%	$2,868	9.03%
Retail trade	44–45	$12,408	14.73%	$4,890	5.81%
Transportation and warehousing	48–49	$3,333	4.86%	$1,541	2.25%
Information	51	$51,097	48.51%	$10,548	10.01%
Finance and insurance	52	$29,116	16.88%	$15,588	9.04%
Real estate and rental and leasing	53	$1,964	1.60%	$739	0.60%
Professional, scientific, and technical services	54	$13,608	42.77%	$5,202	16.35%
Management of companies and enterprises	55	$1,385	31.29%	$644	14.55%
Administrative/support waste management/remediation services	56	$4,116	21.89%	$1,726	9.18%
Educational services	61	$1,997	8.60%	$610	2.63%
Health care and social assistance	62	$14,483	17.29%	$4,005	4.78%
Arts, entertainment, and recreation	71	$1,159	6.18%	$250	1.33%
Accommodation and food services	72	$1,802	4.69%	$716	1.86%
Other services (except public administration)	81	$2,612	8.84%	$874	2.96%
Structure and equipment expenditures serving multiple industry categories		$363	17.45%	$189	9.09%
Total		**$169,812**	**13.29%**	**$63,319**	**4.96%**

Sources: U.S. Census Bureau. "2007 Annual Capital Expenditures Survey: Table 2a. Capital Expenditures and Percent Change for Companies with Employees by Major Industry Sector: 2007, 2006 Revised, and 2005." <http://www.census.gov/csd/ace/xls/2007/Full%20Report.htm>. Released January 22, 2009.
U.S. Census Bureau. "2007 Information and Communication Technology Survey Data Release: Table 3c. Capitalized Expenditures for ICT Equipment and Computer Software for Companies with Employees by Major Industry Sector: 2007, 2006 Revised, and 2005." <http://www.census.gov/csd/ict/xls/2007/Full%20Report.htm>. Released February 26, 2009.

These IT assets are organized into information systems to achieve specific organizational objectives. For instance, accounting and financial management systems maintain the information and applications necessary to effectively track and manage organizations' finances.

Access control decisions can be made and enforced at every level of network architecture: the decision to allow access to a workstation, the decision to allow travel through a router, the decision to allow access to a particular server, and the decision to allow operations on the objects located on the server. Thus, roles can be used to control access to target systems individually, or roles can be created centrally within an IAM application server to manage access across heterogeneous systems.

RBAC can be used by any organization, regardless of size, to specify and administer an access control policy. To the extent that permissions are easily grouped into roles based on business function, location of employee, department, or other attributes of employees, assigning roles to employees rather than individual permissions will yield provisioning and productivity benefits as well as allowing simplified access control policy maintenance and certification. RBAC will yield the greatest provisioning and productivity benefits for organizations with a large number of users occupying relatively stable roles that experience regular turnover.

For any organization that requires regular certification of access control policies, aggregating permissions into roles will simplify and streamline access control policy maintenance and certification. RBAC also allows access control to be managed more directly by the business managers. This creates an important separation of duties, allowing IT professionals to focus on information security design and business managers to govern day-to-day operations.

5. ECONOMIC ANALYSIS METHODOLOGY

This chapter presents the conceptual approach and model used in the economic analysis. Benefits for RBAC-adopting organizations were measured relative to the use of groups, rules, and ACLs, net of ongoing operating costs and one-time adoption costs. A time series of benefits from 1992 through 2009 was calculated by estimating the rate of technology adoption and aggregating benefits across firms and industries. Reducing the time series of economic benefits by the annual costs incurred to develop RBAC and integrate its capabilities into software products equaled net economic benefit estimates. One of the principal findings from the 2002 study was that NIST accelerated the introduction of RBAC by 1 year and reduced development costs. Therefore, benefits attributable to NIST were the difference between the time series of net benefits with and without these acceleration and cost-reduction effects. Thus, there are two bottom-line measures of interest: total net economic benefits of RBAC and net economic benefits of RBAC attributable to NIST.

5.1 Conceptual Approach to Quantifying the Net Economic Benefits of RBAC

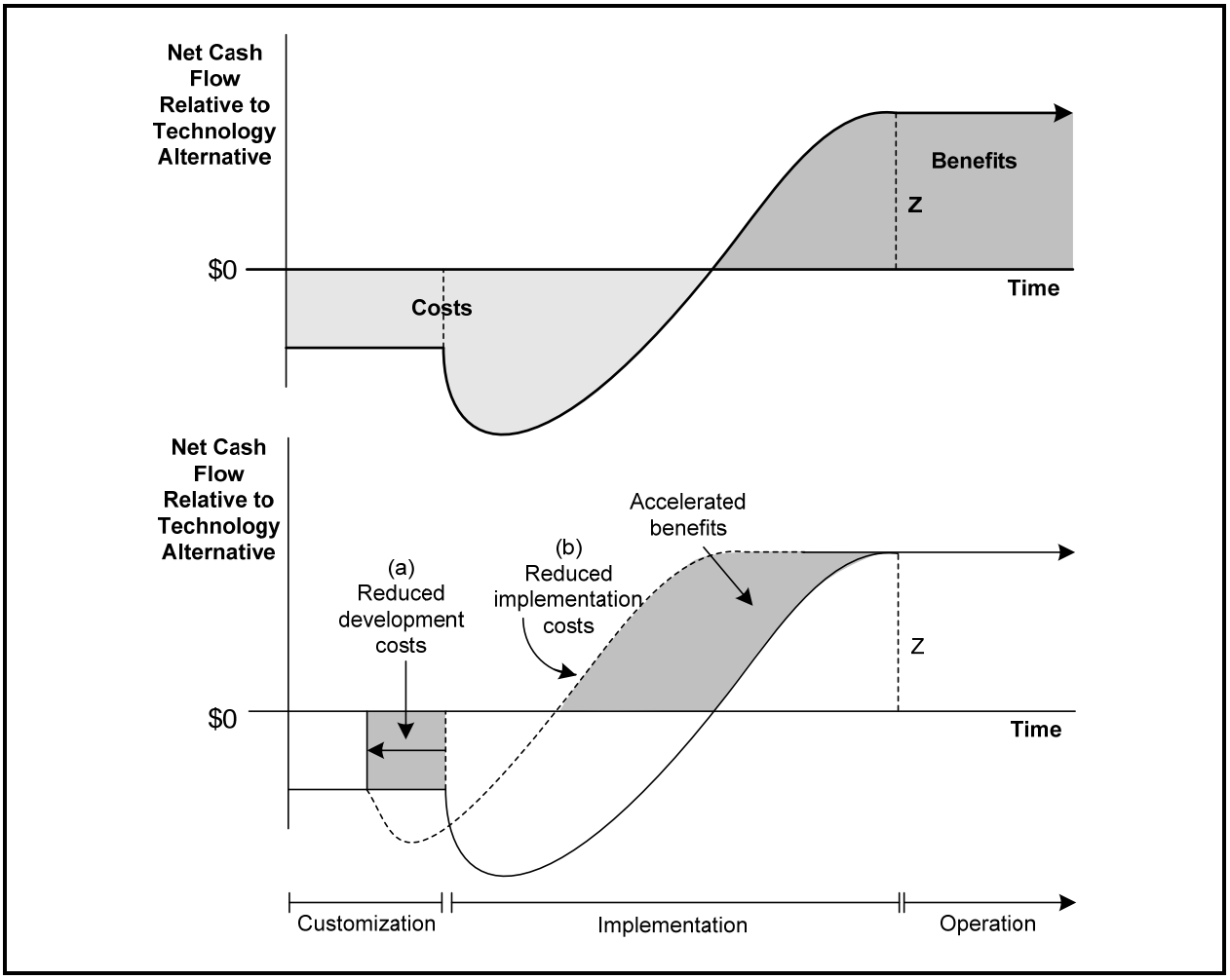
National estimates were the sum of the benefits of each organization using roles to manage all or some of its users' permissions, less costs incurred for designing, implementing, and using RBAC. Setting aside differences in the timing of organizations' RBAC adoption permits one to review the process of modeling benefits and costs through the lens of one hypothetical organization. Figure 5-1 presents a stylized view of how RBAC's costs and benefits accrue over time. The vertical axis represents cash flow relative to ACLs and the horizontal axis represents time.

Three basic periods in an RBAC implementation were pertinent to this analysis:

- System customization refers to a selection and planning period during which necessary IT infrastructure, software systems, and access control policy decisions are made.
- System implementation (integration, testing, and deployment in current parlance) is the period during which software systems are acquired and customized, and roles are tested and refined, as the system is deployed.
- Systems operation refers to normal operation during which time the ongoing benefits from using RBAC policies accrue, relative to using ACLs.

Figure 5-1 illustrates how, over time, the organization moves from an early planning period through a deployment period characterized by increased expenditures for software and services followed by a gradual increase in benefits, net of costs. The routine operation period is represented by a constant net benefit stream. Implicit in this stream is that although there are routine role maintenance and management requirements, under full operation RBAC has net benefits over ACLs.

Figure 5-1. Firm-Level Acceleration of RBAC Adoption Costs and Operating Benefits



In reality, the net benefit stream will likely not accrue as cleanly as presented in Figure 5-1. It is more likely that firms would have a step-wise net benefit curve that may swing intermittently positive and negative. This is in part because best practice in RBAC implementation recommends starting with clearly defined business functions that have relatively static permissions to manage. Even in stable, well-defined job positions where roles are largely static, such as "bank teller," not all permissions can be managed via roles. Roles might be used for some application and business responsibility pairs, but not all. Over time, organizations might gradually extend roles to additional business functions, users, or groups of permissions, thereby creating a step-wise net benefit curve.

For RBAC adopters, the effect of NIST's RBAC development and standardization work is to

- reduce customization costs and time: These cost reductions are shown by the shaded square area (a) in Figure 5-1. Time reductions are shown as a shift in the curve to the left.
- reduce implementation costs and time: The cost reductions are reflected in the nonparallel shift in the implementation stage (b) in Figure 5-1.

For software developers, the effect is analogous to the shaded square (a) in the customization and implementation stages. The availability of the generic technology and standard accelerates product development and reduces development costs.

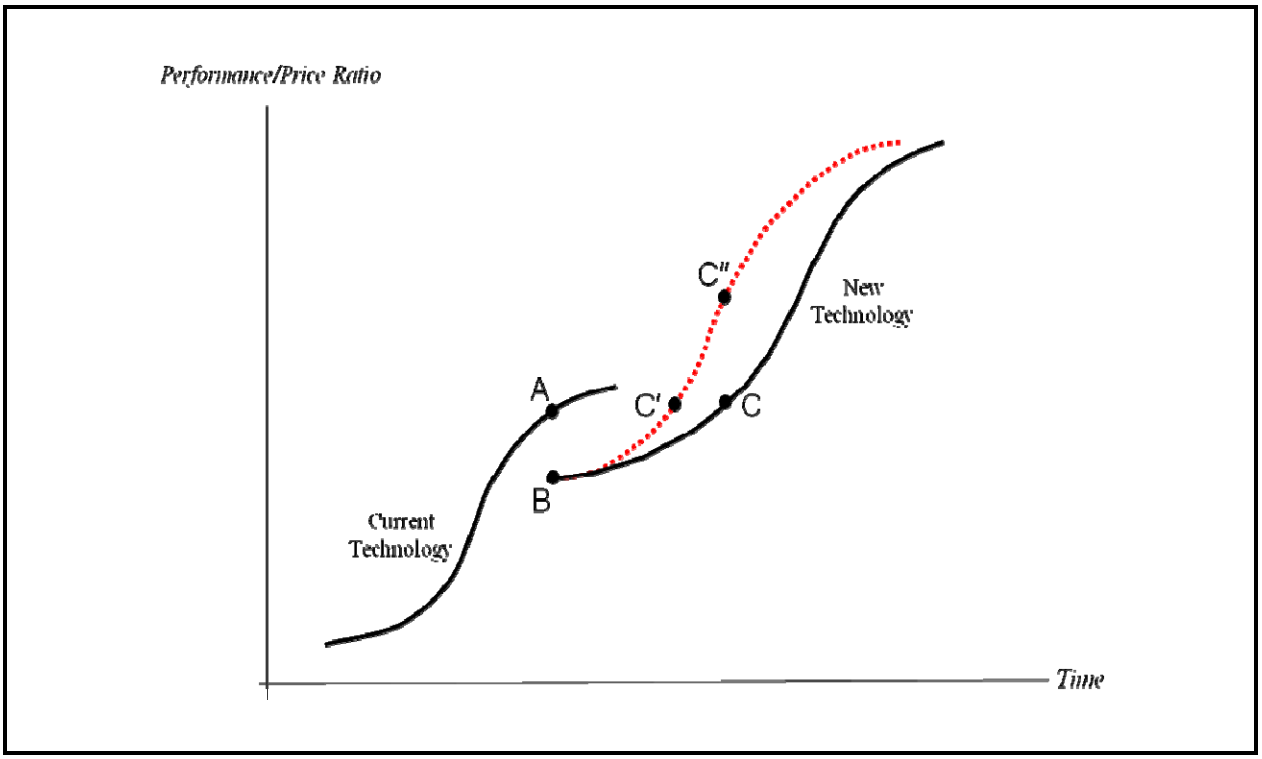
Combined, the two time reductions shift the entire life-cycle curve to the left resulting in the acceleration of benefits.[1] Note that the cost and time effects presented in Figure 5-1 are not mutually exclusive. Lowering the "pull" costs associated with the development, customization, and/or implementation of RBAC can contribute to the acceleration of adoption (not explicitly illustrated in Figure 5-1). It should also be noted in Figure 5-1 that the magnitude of the benefit net of operating costs in the operations stage (Z) remains constant.

Consider now the effect of NIST accelerating RBAC development and adoption. Generic technology development, such as the early NIST RBAC model, is essential to the efficiency of follow-on R&D and rates of innovation. Provision of the generic technology has the effect of raising the performance/price ratio curve for a new technology, which is the equivalent of accelerating market penetration for the new technology (Tassey, 2007). This effect is modeled as the shift from C to C′ in Figure 5-2. The infratechnology attributes of NIST's RBAC standardization work contributes to the upward shift but also contributes a value-added effect, depicted as C′ to C″, by improving the efficiency of R&D, production, and commercialization.

The 2002 study measured the impact of NIST's RBAC activities to have accelerated the adoption of RBAC policies by 1 year. NIST's contributions did not have an impact on the attributes or functionality of the final RBAC systems installed; thus, product quality remains constant and investigations focus on cost and acceleration impacts. Industry experts said that the attributes and features included in the NIST RBAC model would have likely been developed by industry in the absence of NIST, however at a later time and with greater costs.

[1] For simplicity, this discussion ignores the "time value of money" effect due to the acceleration of both the costs and benefits. However, this factor is accounted for in the actual calculation of impact estimates through the appropriate discounting.

Figure 5-2. Effect of Generic Technologies and Infratechnologies



Source: Tassey, G. 2007. *The Technology Imperative*. Northampton, MA: Edward Elgar.

5.2 Economic Benefit and Cost Categories

As reviewed in Chapter 3, RBAC's economic benefits were segmented into five categories (Table 5-1):[2]

- more efficient provisioning by network and systems administrators,
- reduction in new employee downtime from more efficient provisioning,
- more efficient access control policy maintenance and certification,
- enhanced organizational productivity, and
- enhanced system security and integrity.

[2] The 2002 study grouped RBAC's benefits into five general categories with a focus on improved information security and provisioning. Although that study was unable to quantify the benefits of improved security, the study was able to quantify benefits of improved provisioning in terms of both administrative time savings and increased productivity of workers who receive their necessary permissions faster.

Table 5-1. Firm-Level Metrics for Quantifying Economic Benefits

Benefit Category	Technical Measure	Economic Measure	Economic Impact Metric	Unit Scaling Factor
More efficient provisioning by network and systems administrators	Change in administrative time for assigning existing privileges to new users (hours)	Fully loaded cross-industry mean hourly wage rate for network and systems administrators	Change in time required × loaded hourly wage rate	Number of new hires per year
	Changing existing users' privileges (hours)	Fully loaded cross-industry mean hourly wage rate for network and systems administrators	Change in time required × loaded hourly wage rate	Number of internal job changes per year
	Establishing new privileges to existing users (hours)	Fully loaded cross-industry mean hourly wage rate for network and systems administrators	Change in time required × loaded hourly wage rate	Number of new job functions
	Terminating privileges (hours)	Fully loaded cross-industry mean hourly wage rate for network and systems administrators	Change in time required × loaded hourly wage rate	Number of employee terminations per year
Reduction in new employee downtime from more efficient provisioning	Decreased downtime for new employees (hours)	Fully loaded mean hourly wage rate by industry	Percentage loss in productivity × hours × loaded hourly wage rate by industry	Number of new hires per year
More efficient access control policy maintenance and certification	Decreased hours required by IT staff to perform routine policy maintenance and reviews	Average of fully loaded cross-industry mean hourly wage rate for network and systems administrators and computer systems managers	Change in time required × loaded hourly wage rate	Number of employees
	Decreased hours required by business operations staff	Fully loaded cross-industry mean hourly wage rate for managerial occupations	Change in time required × loaded hourly wage rate	Number of employees
	Change in administrative time for compiling permissions inventory (minutes)	Fully loaded cross-industry mean hourly wage rate for network and systems administrators	Change in time required × loaded hourly wage rate	Number of audits and certifications per year
	Reduced time for managers to attest to access privileges (hours)	Fully loaded cross-industry mean hourly wage rate for managerial occupations	Change in time required × loaded hourly wage rate	Number of audits and certifications per year
Enhanced organizational structure	*Organizational efficiency benefits were investigated qualitatively because of great variability in what and how benefits accrue to adopters*			
RBAC reduces the frequency and severity of security violations	*Security benefits were investigated qualitatively because of great variability in what and how benefits accrue to adopters*			

Benefits were calculated on an annualized per-employee basis and then weighted using the shift in the diffusion curve. Economic benefits denominated in labor hours were monetized using mean hourly wage data from BLS (2009). Mean wages were multiplied by 2 to account for employer costs, including expenses for benefits, administrative, and overhead burdens (see Table 5-2).

Economic benefits were reduced by end-user technology adoption costs (Table 5-3). These included all costs directly traceable to implementation of roles, including software customization and installation, systems integration, role engineering, training and education, and all labor activities related to implementation. Research, development, and production of software products are among the most labor-intensive processes in the advanced technology sector. Although it is common for economic analyses to account for transfers of value by netting out product-related revenue, the labor intensity associated with developing and customizing RBAC products and product modules for the enterprise computing market is sufficiently high that expenditures on software products were included. We are overestimating the cost basis, but data were insufficient to resolve value added by different tiers in the value chain. Inclusion of these expenditures further reinforces that net economic benefit estimates and public investment performance measures are conservative.

Data collected via a survey of IAM managers, described later in this chapter, were extrapolated to national impact estimates using Statistics of U.S. Businesses (SUSB) employment data for firms with more than 500 employees (Table 5-4).[3] Recall from Chapter 3 that RBAC is most likely to be used by larger organizations with sufficiently sized user bases to warrant adoption expenses; however, role functionalities are embedded in a large number of software products used by organizations with fewer than 500 employees, suggesting that net benefits may be an underestimate. Smaller organizations may indeed use RBAC; however, primary data collection and secondary research on usage trends among smaller organizations were insufficient to estimate adoption, usage, and benefits. Thus, the estimates presented in this report may be considered conservative even though they are the best possible estimates given data limitations.

To minimize survey respondent burden, we assumed that survey respondents' historical staffing growth rates reflected prevailing industry employment trends. This assumption avoided the need to ask respondents to provide annual employment data for the past decade. Between 1998 and 2008, several sectors experienced significant changes in employment. For example, professional, scientific, and technical services increased over 1 million employees, or 52%, since 1998. In addition, the retail trade sector, which employed over 9 million people, was not included in the first study but was included in this retrospective analysis. Anecdotal evidence

[3] The first study used 1998 SUSB employment data by sector—the last year for which data were then available—and assumed these values would be fixed over time, only varying the adoption rate. This study used actual annual data for 1998 through 2009.

Table 5-2. Fully Loaded Mean Hourly Wage Rate, by Industry

NAICS	Sector	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
22	Utilities	42.60	44.49	45.41	46.01	60.85	60.34	58.52	56.63	56.90	57.40	58.73	59.16
23	Construction	40.41	43.79	43.67	43.87	45.03	44.80	44.04	43.17	42.82	42.96	43.76	44.72
31-33	Manufacturing	38.83	40.54	41.41	42.20	42.27	42.75	42.07	41.37	41.15	41.43	41.98	42.86
42	Wholesale trade	40.87	42.93	43.93	44.45	46.90	47.15	46.21	45.75	45.86	46.51	47.25	48.00
44-45	Retail trade	23.41	24.78	24.77	25.17	28.93	28.94	28.39	27.78	27.60	27.57	27.71	27.58
48-49	Transportation and warehousing	42.60	44.49	45.41	46.01	41.99	42.96	42.16	41.70	41.17	41.27	41.07	41.12
51	Information	37.56	39.25	40.36	40.85	53.77	53.86	53.51	52.75	52.93	54.14	55.62	56.80
52	Finance and insurance	43.30	47.38	47.96	47.97	52.65	52.40	52.20	51.85	52.21	52.74	53.79	54.62
53	Real estate and rental and leasing	43.30	47.38	47.96	47.97	36.28	36.55	36.22	36.74	36.77	37.10	37.56	38.32
54	Professional, scientific, and technical services	37.56	39.25	40.36	40.85	62.73	63.16	62.59	61.71	61.85	62.84	64.08	65.62
55	Management of companies and enterprises	43.30	47.38	47.96	47.97	59.76	59.92	59.81	59.48	60.32	61.73	63.19	64.78
56	administrative and support and waste management and remediation services	37.56	39.25	40.36	40.85	30.16	31.27	30.72	31.11	30.91	31.16	31.67	32.34
61	Educational services	37.56	39.25	40.36	40.85	44.69	44.96	44.31	44.11	44.46	44.59	45.53	46.18
62	Health care and social assistance	37.56	39.25	40.36	40.85	41.73	42.24	41.73	41.52	41.91	42.24	43.01	43.68
71	Arts, entertainment, and recreation	37.56	39.25	40.36	40.85	30.03	30.36	29.77	29.44	29.87	30.07	30.44	30.82
72	Accommodation and food service	23.41	24.78	24.77	25.17	21.10	20.92	20.52	20.13	20.06	20.36	20.71	21.12
81	Other services (except public administration)	37.56	39.25	40.36	40.85	32.60	32.62	32.40	32.36	32.34	32.55	32.98	33.52
92	Public administration	42.94	44.62	45.70	46.19	46.70	47.32	46.92	46.65	46.98	47.44	48.06	49.24

Source: Bureau of Labor Statistics, Department of Labor, 2010. "Occupational Employment Statistics (OES) Survey: National Cross-Industry Estimates 1998-1999. Accessed September 20, 2010. http:/stat.bls.gov/oes/home.htm.

Notes: All dollar values have been adjusted to real 2009 dollars using the gross domestic product (GDP) implicit price deflator (BEA, 2009). Fully loaded wage rates are two time the average wage rate to incorporate other costs of employment. Wages between 1998 and 2001 are based on SIC code divisions to provide the appropriate NAICS sector estimate.

Table 5-3. Firm-Level Metrics for Quantifying Adoption and Implementation Costs

Cost Category	Technical Measure	Economic Measure	Economic Impact Metric
IT, security, and/or audit staffing for RBAC policy design and implementation	FTE assigned from IT group	Average of fully loaded cross-industry mean hourly wage rate for network and systems administrators and computer systems managers	Number of FTE × 2000 hours × loaded hourly wage rate
Business group staffing for RBAC policy design and implementation	FTE assigned from business operations	Fully loaded cross-industry mean hourly wage rate for managerial occupations	Number of FTE × 2000 hours × loaded hourly wage rate
Expenditures on third-party systems integration, services, and role engineering, specific to RBAC implementation			Total cost
Expenditures on software solutions or modules specific to RBAC implementation			Total cost[a]
Expenditures on hardware specific to RBAC implementation			Total cost[a]
Annual licensing agreements and fees for software systems specific to RBAC implementation			Annual cost[a]

[a] Although it is common for economic analyses to account for transfers of value by netting out product-related revenue, the labor intensity associated with developing and customizing RBAC products and product modules for the enterprise computing market is sufficiently high that expenditures on software products were included. Inclusion of these expenditures further reinforces that net economic benefit estimates and public investment performance measures are conservative.

suggested that the retail sector, which has stable job positions, high turnover, and large numbers of employees within a small number of job categories, has been active in RBAC adoption.

5.3 Economic Costs of Developing RBAC and Including RBAC in Software Products

RBAC development costs consisted of those incurred by NIST, other standards and technology development groups, and software developers and integrators. NIST expenditures on RBAC initiatives totaled $2.6 million between 1992 and 2002 (negligible amounts were expended in recent years).[4] The technical and economic impact metrics for NIST's acceleration effect were the average number of months an adoption decision was advanced and the value of the benefits of RBAC realized as a result of the acceleration.

Software developers' costs were estimated to be approximately $6.2 million per year through 2006 to incorporate RBAC functionality into software products, according to findings

[4] For 2002 through 2006 most NIST activities focused on supporting and revising standards and providing implementation guidance in response to industry's challenges associated with adopting role-based policies. Consequently, NIST's efforts between 2006 and 2009 fall largely in the realm of implementation assistance. NIST has been working with other thought leaders as part of the INCITS groups to provide RBAC implementation and role-engineering guidance to the end-user community, software developers, and systems integrators.

Table 5-4. Employment in Organizations with More than 500 Employees, by Industry

NAICS	Sector	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007
21	Mining	278,652	260,594	255,654	271,026	261,480	253,576	259,156	277,537	309,795	418,609
22	Utilities	578,717	564,707	550,494	548,514	537,664	532,443	527,221	523,931	505,268	512,412
23	Construction	679,003	774,783	897,732	964,696	946,025	894,227	902,043	939,576	1,074,142	1,077,482
31–33	Manufacturing	9,931,342	9,818,591	9,672,109	9,312,458	8,298,668	8,030,010	7,741,481	7,628,545	7,575,462	7,402,462
42	Wholesale trade	2,035,377	2,137,745	2,225,508	2,277,095	2,180,763	2,223,480	2,269,755	2,331,700	2,344,969	2,329,016
44–45	Retail trade	7,851,673	8,094,491	8,349,169	8,427,885	8,458,586	8,463,187	8,879,752	9,030,694	9,453,604	9,621,300
48–49	Transportation & warehousing	1,955,724	2,102,888	2,233,906	2,192,925	2,089,679	2,515,586	2,527,922	2,581,515	2,676,777	2,777,353
51	Information	2,238,831	2,321,039	2,549,220	2,759,701	2,632,117	2,678,380	2,563,528	2,512,310	2,502,240	2,522,129
52	Finance & insurance	3,889,704	4,048,969	4,049,152	4,307,387	4,451,290	4,399,089	4,373,555	4,302,969	4,463,233	4,414,232
53	Real estate & rental & leasing	504,670	550,131	584,186	632,766	630,317	628,651	643,991	681,017	695,767	720,696
54	Professional, scientific, & technical services	2,040,933	2,242,784	2,407,973	2,567,560	2,523,201	2,793,556	2,909,470	2,948,040	3,096,079	3,184,574
55	Management of companies & enterprises	2,399,500	2,474,610	2,565,880	2,553,750	2,536,367	2,530,947	2,482,233	2,518,437	2,563,968	2,737,814
56	Administrative & support & waste management & remediation serv	4,426,750	4,989,739	5,660,629	5,536,302	5,013,669	5,045,753	5,125,110	5,660,565	6,271,088	6,259,488
61	Educational services	1,231,030	1,288,503	1,339,116	1,375,349	1,426,573	1,471,203	1,563,695	1,584,946	1,645,568	1,675,703
62	Health care & social assistance	7,304,840	7,354,644	7,401,086	7,628,901	7,755,218	8,012,865	8,149,160	8,276,386	8,504,967	8,807,758
71	Arts, entertainment, & recreation	475,632	506,624	558,392	587,284	607,866	596,281	609,820	655,818	675,571	695,324
72	Accommodation & foodservices	3,658,508	3,789,408	3,926,848	3,973,106	3,962,289	4,090,179	4,182,144	4,414,317	4,532,320	4,710,142
81	Other services (except public administration)	688,460	723,058	748,720	776,852	750,209	731,041	743,650	777,986	794,978	842,853
92	Public Administration (federal government)	2,447,496	2,449,089	2,425,898	2,411,630	2,426,467	2,453,158	2,445,287	2,437,558	2,438,657	2,462,127
	Total	54,616,842	56,492,397	58,401,672	59,105,187	57,488,448	58,343,612	58,898,973	60,083,847	62,124,453	63,171,474
	Total of Included Sectors	40,714,035	41,550,244	42,276,837	42,980,616	42,048,622	42,384,693	42,776,374	43,010,883	44,000,596	44,469,890

Source: U.S. Census Bureau, Statistics of U.S. Businesses. 2010. "Number of Firms, Number of Establishments, Employment and Annual Payroll by Employment Size of the Enterprise for the United States, All Industries: 1998-2007." Accessed October 16th, 2009 and September 17th, 2010. http://www.census.gov/econ/susb/.

U.S. Census Bureau, Government Employment and Payroll. 2010. "Federal Government Civilian Employment: Total Full-Time Employees. 1998-2007."Accessed September 29, 2010. http://www.census.gov/govs/apes/.

from the 2002 study. This cost would have been $6.8 million in the absence of NIST's research. Thus, actual costs were 92% of what they would have been.[5] Industry experts consulted during the first study indicated that virtually all the R&D and implementation costs were in the form of staff time. Therefore, the technical and economic impact metrics are primarily in terms of changes in labor hours and labor expenditures, respectively. Changes in R&D expenditures per company were averaged and then weighted by the number of software companies developing RBAC products and large companies developing in-house RBAC systems.

The 2010 update did not reevaluate software developers' costs because costs incurred in more recent years likely relate to new innovations or extensions of capabilities. This study assumes that development costs were stable over time and extended annual costs through 2009. In real terms (2009$), RBAC development costs were estimated to be $69 million.

5.4 Model for Quantifying RBAC's Economic Impacts

The benefits of RBAC, as described in Table 5-1, are defined as the flow of operating benefits (OB) over time. Benefits are expressed per employee and may vary by industry, *i* indexes industry, and *t* indexes year:

$$OB_{it} = PB_{it} + DB_{it} + AB_{it} + SB_{it} \quad (5.1)$$

where

OB_{it} = total operating benefits per employee

PB_{it} = provisioning cost reductions per employee

DB_{it} = productivity benefits per employee, including reduced employee downtime

AB_{it} = access control policy maintenance, audit, and certification benefits per employee

SB_{it} = security benefits per employee

Implementation costs are also expressed as expenditures per employee for a given industry:

IC_{it} = RBAC user customization and implementation costs per employee

Finally, RBAC development costs are expressed as average software developer R&D expenditures and average user R&D expenditures over time:

[5] These estimates were confirmed with software developers. The original estimate deemed to be accurate given that it was developed concurrently with early integration of RBAC into commercial products. The 2002 study estimated costs to be $5.05 million per year (2000 dollars), or $6.24 million per year in 2009 dollars. The counterfactual cost without NIST was estimated to be $5.5 million per year (2000 dollars), or $6.80 million in 2009 dollars.

R&Dsd = total R&D costs for a typical software development company for implementing RBAC concepts into their products[6]

R&Dih = total R&D costs for a typical user for integrating RBAC concepts into their in-house systems

The time series of net benefits (NB_t) from RBAC can then be calculated by summing across the costs and benefits to software developers and users in all industries:

$$NB_t = \sum^{i} (OB_{it} - IC_{it}) * Emp_{it} - (R\&Dsd * Nsd_t + R\&Dus * Nih_t), \quad (5.2)$$

where

Nsd_t = number of software developers in year *t* that developed an RBAC product

Nih_{it} = number of users in industry *i* that developed in-house RBAC products in year *t*

Emp_{it} = number of employees in industry *i* being managed using RBAC systems in year *t*

The net benefits are separated between the one-time reduction in development and implementation costs and the continuing operational and administrative benefits. Note that the end-user benefits are a function of the cumulative number of employees being managed by an RBAC system, whereas the end-user costs represent the incremental number of employees brought on to RBAC systems.

The economic impact of NIST/ITL's RBAC project results from changes in R&D costs, changes in implementation costs, and changes in the number of employees being managed by RBAC systems over time. This is expressed as

$\Delta R\&Dsd$ = change in R&D costs for software developers

$\Delta R\&Dus$ = change in R&D costs for users developing in-house RBAC systems

ΔIC_{it} = change in implementation costs

ΔEmp_{it} = change in the number of employees being managed by RBAC systems

Rewriting Equation (5.2) in terms of changes resulting from NIST's contributions yields

$$\Delta NB_t = \sum^{i} [OB_{it} - (IC_{it} - \Delta IC_{it})] * \Delta Emp_{it} - (\Delta R\&Dsd * Nsd_t + \Delta R\&Dus * Nih_t). \quad (5.3)$$

Three benchmark measures—benefit-to-cost ratio (BCR), net present value (NPV), and internal rate of return (IRR)—were used to evaluate the time series of quantified benefits and costs.

[6] R&D costs are allocated to the initial year of RBAC system development. Industry experts indicated that NIST's impact on the development process typically occurred early in the project; hence, any impact on R&D expenditures was likely to be realized in the first year.

- **Benefit-to-Cost Ratio**: The BCR calculated in this analysis is the ratio of the NPV of benefits to the NPV of costs, which accounts for differences in the timing of cash flows (which has implications for the discounted value of $1 in one time period versus another).

  Because benefits and costs occur at different time periods, both are expressed in present-value terms before the ratio is calculated. Essentially, a BCR greater than 1 indicates that quantified benefits outweigh the calculated costs. A BCR less than 1 indicates that costs exceed benefits, and a BCR equal to 1 means that the project broke even.

- **Net Present Value**: In this study, the discount rate was set at 7%, the Office of Management and Budget (OMB)-specified level.[7] Any project that yields a positive NPV is considered economically successful. Projects that show a positive NPV when analyzed using OMB's 7% real discount rate are socially advantageous. A negative NPV would indicate that the costs to society outweigh the benefits, and an NPV equal to zero would indicate a breakeven point.

  This study sets the base year for the NPV calculation to 2000 in order to align with the NPV forecasts presented in the 2002 study.

- **Internal Rate of Return**: The IRR on an investment should be interpreted as the percentage yield on an R&D project over the life of the project, often multiple years. In mathematical terms, the IRR is the discount rate that sets the NPV equal to zero or results in a benefit-cost ratio of 1.

  It should be noted that the IRR was not able to be calculated in this analysis because of intermittent negative cash flows in the time series of net economic benefits attributable to NIST.

5.5 Primary Data Collection

To estimate economic benefits, and activities, primary data from stakeholders throughout the RBAC value chain included a survey of IAM managers. A principal focus of early primary data collection was to engage each tier of the access control value chain—from developers through end users—to ensure that a complete taxonomy of economic benefit and costs categories was developed. Extensive discussions with IAM experts and managers were held to develop hypotheses about impact categories, review adoption drivers, and characterize adopting firms. This process was necessary to form the basis against which economic benefits might be quantified. Experts were from a diverse group of stakeholders, including technology research groups, government and university research centers, systems integrators, auditors, health systems, and large financial corporations.

One of the principal outcomes from these interviews was the development of a survey instrument, included as Appendix A, for end users that RTI fielded with outreach support from

[7] See OMB Circular A-94.

the Burton Group (now part of Gartner), ISACA, and several IT blogs. Survey data were collected between July and September 2010.

Companies responding to the internet survey and/or participating in in-depth interviews employed 2 million (4.5%) of the estimated 44.5 million people employed by organizations with more than 500 employees in 2010. Table 5-5 presents the industry distribution of more than 150 responding firms supplying sufficient information to be included in the economic analysis.[8] In addition to these firms, the results represent the views of 22 software developers and systems integrators and 9 professional societies and technology research groups.

The survey requested that respondents provide the

- number of people employed by their organization;
- number of user accounts for their intranets;
- whether they use roles and how they implemented roles;
- their access control approaches by system;
- percentage of their organizations' users with at least some of their permissions managed by roles biannually between 1999 and 2010;

Table 5-5. Distribution of Survey Respondents, by Industry

Sector	Sample Percentage
Finance and insurance	24%
Information	19%
Health care and social assistance	12%
Public administration	11%
Professional, scientific, and technical services	9%
Educational services	6%
Utilities	5%
Other services (except public administration)	5%
Manufacturing	5%
Retail trade; arts, entertainment, and recreation; and wholesale trade	<5%

[8] In the 2002 study, retail and wholesale trade were both excluded from our extrapolation of RBAC benefits. Based on their responses to the survey, we have included the sectors in our benefits extrapolation for this study. Conversely, the transportation and warehousing sector was included in the previous RBAC study, but no representative company from that sector responded to the survey, so we have excluded the sector from the current study's benefits extrapolation.

- percentage of these users' permissions managed by roles biannually between 1999 and 2010;[9]
- RBAC implementation costs, if applicable;
- provisioning costs and benefits (with and without RBAC);
- reduced employee downtime (with and without RBAC); and
- access control policy maintenance and certification activities and level of effort (with and without RBAC).

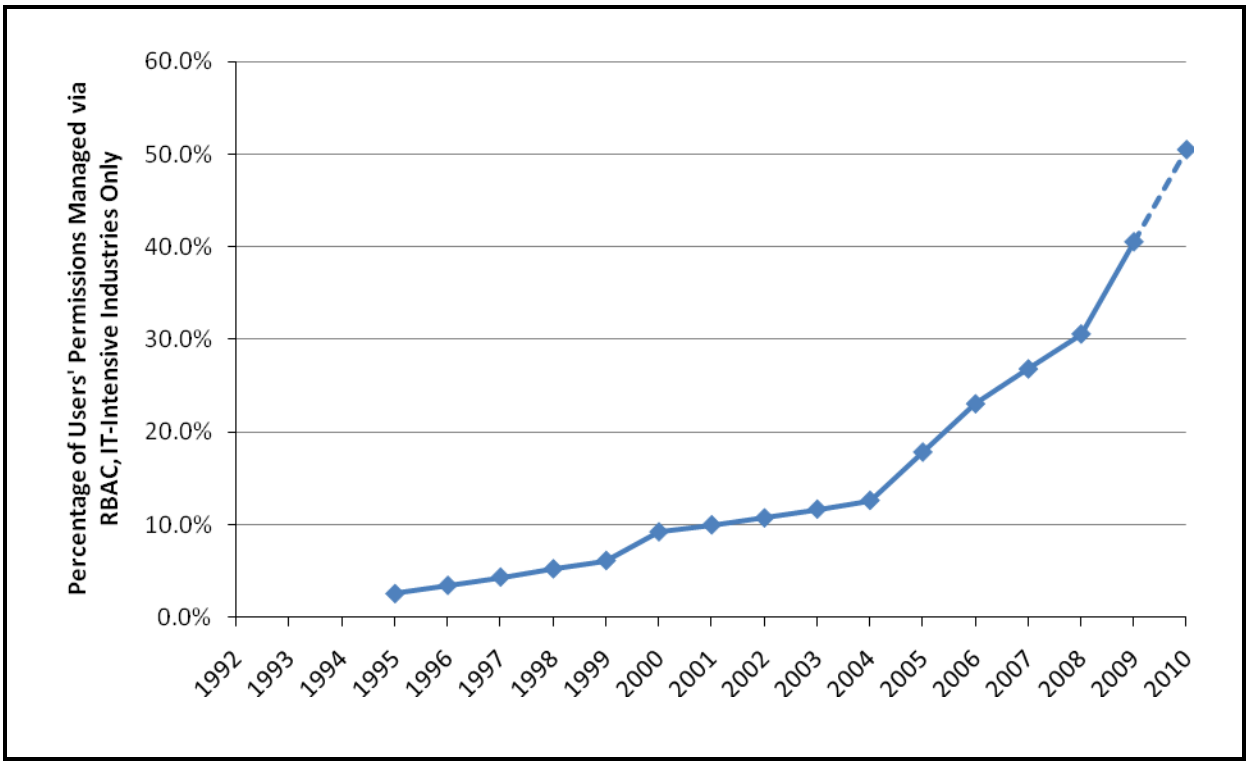
[9] To minimize respondent burden and avoid requesting RBAC usage data by year, biannual estimates were requested. Intervening years were calculated by taking the midpoint between respondents' data entries.

6. ECONOMIC ANALYSIS RESULTS

This analysis estimates that between 1994 and 2009 RBAC generated $11 billion in cost savings for American businesses. Cost savings were offset by $5 billion in software expenditures and systems integration fees to yield economic benefits net of adoption costs of $6 billion.

The use of roles has grown steadily since 1994, with the rate of adoption accelerating in 2004 and again in 2008. The number of employees who had at least some of their permissions managed via roles grew from 2.5% in 1995 to 40.5% in 2009, and we estimate that by the close of 2010 that figure will grow to 50.5%. By the end of the time period illustrated in Figure 6-1, we estimate that just over 50% of users at organizations with more than 500 employees are expected to have at least some of their permissions managed via roles (see also Table 6-1). NIST's role in accelerating the development of RBAC models (generic technology) and supporting and leading RBAC-related standardization efforts (infratechnology) hastened RBAC's introduction into software products by 1 year and lowered development costs. The time series of net economic benefits attributable to NIST totaled $1.1 billion.

Figure 6-1. RBAC Adoption, 1992–2010



Note: Industries were defined by 2-digit NAICS code and included utilities; manufacturing; wholesale trade; retail trade; information; finance and insurance; professional, scientific, and technical services; educational services; health care and social assistance; arts, entertainment, and recreation; other services; and public administration.

Table 6-1. RBAC Adoption and Employment Data

Year	Employment in Selected Industries, Organizations >500 Employees[a]	RBAC Adoption	Estimated Employment with at Least Some Permissions Managed via Roles	Estimated Number of Public Companies Using Roles for Certification and Attestation
1994	40,714,035[e]	*	*	*
1995	40,714,035[e]	2.5%	1.0	101
1996	40,714,035[e]	3.4%	1.4	137
1997	40,714,035[e]	4.3%	1.8	173
1998	40,714,035	5.2%	2.1	208
1999	41,550,244	6.1%	2.5	244
2000	42,276,837	9.2%	3.9	368
2001	42,980,616	10.0%	4.3	398
2002	42,048,622	10.7%	4.5	428
2003	42,384,693	11.7%	4.9	465
2004	42,776,374	12.6%	5.4	503
2005	43,010,883	17.8%	7.7	711
2006	44,000,596	23.0%	10.1	919
2007	44,469,890	26.8%	11.9	1,070
2008	44,469,890[e]	30.6%	13.6	1,220
2009	44,469,890[e]	40.5%	18.0	1,617
2010	44,469,890[e]	50.5%	22.5	2,015

* Data for 1994 and earlier are unreliable because of very low levels of RBAC usage.

[a] Industries were defined by 2-digit NAICS code and included utilities; manufacturing; wholesale trade; retail trade; information; finance and insurance; professional, scientific, and technical services; educational services; health care and social assistance; arts, entertainment, and recreation; other services; and public administration. This time series was not collected by NAICS for 1994 through 1997 and was not yet available for 2008 through 2010. Data for 1998 were used for 1994 through 1997 and data for 2007 were used for 2008 through 2010.

Source: U.S. Census Bureau, Statistics of U.S. Businesses. 2010. "Number of Firms, Number of Establishments, Employment and Annual Payroll by Employment Size of the Enterprise for the United States, All Industries: 1998-2007." Accessed October 16th, 2009 and September 17th, 2010. http://www.census.gov/econ/susb/. Wilshire Associates Incorporated. 2010. "The Wilshire 5000 Total Market Index: Fundamental Characteristics." Accessed October 16, 2009. http://www.wilshire.com/Indexes/Broad/Wilshire5000/Characteristics.html.

6.1 Trends in Role Use and Access Control Policy Approaches

Our survey of identity and access control managers captured a wealth of information on the use of roles, including adoption rates, key business drivers, and perceptions of utility and benefit.

6.1.1 RBAC Adoption, 1994 to 2009

Although the RBAC model was published in 1992 and we have information that some companies were using roles before 1995, we were not able to reliably estimate penetration for

this period. For 1995 we estimated just under a 4% penetration rate, growing to about 11% in 2002, 13% in 2004, and 41% in 2009.[1] This estimate is consistent with the regulatory drivers during this period as well as increasing role functionality native within common applications and systems, such as Active Directory and Oracle Database 11g.

Most respondents reported that implementing roles has been a gradual process, with applications and user groups migrating to roles in a multiphase process, often as part of broader IT initiatives. One manager noted that "current work to consolidate and standardize systems and applications has led to a push to more efficiently and effectively manage user access. We have migrated toward a role-based user management approach."

To extrapolate benefit-cost estimates from the survey sample to national estimates, we assume that this adoption curve represents a cross-industry average for all organizations in IT-intensive industries with more than 500 employees (see Section 5.5).[2]

6.1.2 Respondents' Views on the Business Case for RBAC

Whereas Chapter 3 reviewed RBAC's advantages from the vantage point of role characteristics and access control theory, our survey collected IT managers' reasons for managing authorizations using roles. In their own words, the fundamental drivers for and advantages of RBAC were as follows:

- Congruence between business processes and access controls.
- Ability to relate access policies to authorizers more easily via business roles instead of functional permission names (e.g., mainframe transaction name). Without this, revalidation of access rights is both too costly and too time consuming to carry out effectively.
- Compliance with Sarbanes-Oxley and other federal regulations.
- Ease of oversight and audit of appropriate access (traceability).
- Greater efficiency in provisioning and deprovisioning.
- Separation of duties.
- Ease, yet compliance of appropriate access levels to enterprise systems and data.
- Data ownership considerations.
- Information protection, confidentiality, and integrity.

[1] Survey respondents provided information regarding both the number of employees managed using RBAC and the percentage of these employees' permissions managed using roles. These two values were combined to estimate the total universe of user permissions that were managed using roles from 1999 to 2010. Data from the 2002 study were merged into this study's data set, permitting the estimation of RBAC adoption between 1995 and 1999. To minimize respondent burden and avoid requesting RBAC usage data by year, biannual estimates were requested. Intervening years were calculated by taking the midpoint between respondents' data entries.

[2] Industries were defined by 2-digit NAICS codes and included utilities; manufacturing; wholesale trade; retail trade; information; finance and insurance; professional, scientific, and technical services; educational services; healthcare and social assistance; arts, entertainment, and recreation; other services; and public administration.

Roles are most important for risk-based, mission-critical financial and accounting systems or niche, functional applications like call-center operations. Nearly all the comments received focused on more efficient provisioning, easier access control policy maintenance, and compliance and certification. No respondent reported that they were able to most closely align their IT infrastructure to their business operations. However, because it was not explicitly reported in qualitative responses does not necessarily mean that such benefits do exist.

Over 80% reported that using roles improved the efficiency of maintaining their organization's access control policy, a qualitative assessment that is consistent with the economic analysis results presented later (Table 6-2). These organizations were more likely to

- use roles that were native to applications and systems than they were to engineer their own roles (78% vs. 22%),
- use enterprise roles via an identity management solution that manages permissions for users across multiple applications and/or systems (54% vs. 46%), and
- encounter challenges because of a lack of standardization in roles or specifications across different applications and systems (55% vs. 45%).

Standardization remains an issue. Although progress has been made in standardizing access control infrastructure, issues with system and application interfaces, a lack of common role definitions, and the exchange of permissions across information systems remain challenges.

6.1.3 Respondents' Views on Barriers to RBAC Implementation

In their remarks, respondents often expressed a preference for RBAC but were faced with the reality of business operations, applications, and systems that were inhospitable to it or for which RBAC would be counterproductive. The three most common barriers were the following:

- Certain combinations of user types, systems, and workflows do not lend themselves to effective management via roles.

Table 6-2. Adopters' Experiences with RBAC

Question	Yes	No
Has the use of roles improved the efficiency of maintaining your organization's access control policy?	84%	16%
Do you use roles that are native within applications?	78%	22%
Do you use enterprise roles via an identity management solution that manages permissions for users across multiple applications and/or systems?	54%	46%
Does your organization run an enterprise resource planning (ERP) system (i.e., Oracle, SAP)?	54%	46%
Has your organization encountered any challenges with routine provisioning because of a lack of standardization in roles or specifications across different applications or systems?	55%	45%

- Legacy systems were not designed with sufficiently granular levels of authorization to be compatible with roles.
- RBAC implementation was perceived to be a significant investment of human resources, capital, and time, competing with other IT projects for limited resources.

The most common response during our telephone interviews with IT managers was that, although many users and permissions fit well within static role definitions, there will always be a portion of users and permissions for which the costs of role definition and maintenance are prohibitive. Even a respondent whose organization has a highly centralized IAM solution reported that although "[r]oles are standard, other means are used when they do not easily interface with our centralized approach."

Roles could become counterproductive because in many scenarios there would be too many exceptions. Indeed, one responding organization had developed so many roles that role assignment and maintenance became an unexpected burden.

Further, many IT managers said that a mix of legacy system issues and a history of ad-hoc approaches to policy design precluded a move toward RBAC. An illustrative comment was that "[o]ur environment is realistically more complex than this [survey] allows for; there are hundreds of applications, and increasingly we are trying to move to [RBAC], but few systems have this as of yet, and ACLs are the general answer."

Many legacy systems do not support role-based methods because they were not designed with sufficiently granular multiuser and multilevel access in mind. Both latest generation and legacy systems may be maintained by third parties, adding an additional layer of complexity to any desired migration to RBAC.

Implementing RBAC can be expensive, and "retrofitting" systems and in-house code requires technical talent, time, and funds, competing with other business imperatives for budget. Jettisoning legacy systems and applications was not going to happen, and the consequence, as far as access control is concerned, is often a patchwork of approaches or large numbers of ACLs that must be maintained. These situations were not reported as being ideal, but more a matter of tacit acceptance of ongoing costs to avoid what are thought to be substantial one-time investments for revamping systems'.

6.1.4 Prevalence of Role Use by System Type

Survey respondents provided a wealth of information about how they manage access to 12 common information systems. They first reported the primary mechanism they used for each system (Table 6-3); then they were provided the opportunity to report whether they used a combination of mechanisms, often referred to as a hybrid approach.

Table 6-3. Primary Access Control Mechanism Used, by Information System Category

System	ACLs	Roles	Rules	Attributes	Open Access
Human resource information systems	37%	56%	6%	2%	0%
Sales and customer relationship management systems	41%	52%	2%	4%	0%
Accounting and financial management systems	41%	50%	6%	2%	2%
Purchasing, order management, and logistics systems	41%	50%	7%	2%	0%
Business process management systems	42%	44%	7%	4%	2%
Enterprise database systems	43%	41%	10%	6%	0%
Electronic health record and health information systems	48%	34%	10%	7%	0%
Identity management systems	39%	34%	15%	7%	5%
Physical security services	50%	28%	9%	9%	4%
Directory services	49%	27%	10%	6%	8%
Network identity services	53%	22%	14%	6%	4%
Web services	51%	20%	14%	6%	8%

Roles were most likely to be used as the primary access control mechanism for

- human resource information systems (56%);
- sales and customer relationship management systems (52%);
- purchasing, order management, and logistics systems (50%);
- accounting and financial management systems (50%); and
- business process management systems (44%).

6.1.5 Prevalence of Hybrid Access Control Approaches

Organizations reporting hybrid approaches almost entirely reported using roles as the primary mechanism and ACLs as the secondary one, or ACLs as primary followed by roles as secondary. As one respondent noted, "While we attempt to build RBAC controls, they tend to be implemented by using 'groups'; hence the separation of ACL and RBAC is difficult as they tend to overlap." Table 6-4 presents information on hybrid approaches that were almost exclusively either

- use of ACLs as the primary mechanism and roles as a secondary mechanism, or
- use of roles as the primary mechanism and ACLs as a secondary mechanism.

Interestingly, for those organizations with electronic health records and health information systems, the largest percentage of respondents with these systems (48%) reported

Table 6-4. Hybrid Access Control Approaches, by Information System Category

System	Respondents that Primarily Use ACLs That Reported Roles as a Secondary Mechanism	Respondents that Primarily Use Roles That Reported ACLs as a Secondary Mechanism
Accounting and financial management systems	44%	53%
Electronic health record and health information systems	60%	50%
Business process management systems	46%	54%
Sales and customer relationship management systems	33%	50%
Human resource information systems	53%	67%
Directory services	57%	56%
Identity management systems	27%	38%
Purchasing, order management, and logistics systems	50%	40%
Physical security services	36%	45%
Network identity services	56%	40%
Web services	43%	43%
Enterprise database systems	46%	62%

using ACLs as their primary access control mechanism. We had expected roles to be the largest percentage because a 2009 survey conducted by the Healthcare Information and Management Systems Society (HIMSS) reported that 76% of health care organizations used RBAC (HIMSS, 2009). We estimated 34%. In follow-on questioning, however, 60% of respondents that primarily use ACLs also reported using roles as a secondary mechanism for these systems. Conversely, when roles were the primary mechanism, half of respondents stated they also used ACLs (Table 6-4). Thus, our survey results are in the same overall range and confirm HIMSS's findings that roles are used extensively in the health care sector. A review of responses for EHRs also points to the prevalence of hybrid approaches. Only about one-third of large organizations with these systems use roles, and of these only about half use roles.

6.2 Quantified Benefits from More Efficient Provisioning by Network and Systems Administrators

In terms of quantified benefits, provisioning benefits manifest in two ways: cost savings from provisioning activities by network and systems administrators and cost savings from reduced employee downtime.

A small proportion of the economic benefits we quantified were related to provisioning activities conducted by network and systems administrators. Indeed, we estimate that for a company with 10,000 employees savings on IT department labor from streamlined provisioning alone were about $24,000 per year, which is less than 10% of the benefit accruing from reducing

the period during which any given user is underentitled.[3] (Note that benefits for reduced employee downtime and easier access control policy maintenance were calculated and are presented separately in the follow sections.)

Table 6-5 presents cross-industry savings for network and systems administrators using industry averages. For each of four provisioning tasks—assigning, changing, establishing, and terminating permissions—we compared the time requirement with and without roles to accomplish the task. For example, terminating permissions for the typical employee required 4.7 minutes using roles compared to 7.6 minutes using ACLs.

The net time savings were then multiplied by the number of times those tasks took place to estimate time savings for administrators in a typical year. The cross-industry average turnover ratio for terminations per employee was 0.17, meaning that an organization with 100 employees would expect to deprovision 17 times per year. On average, the total savings per employee per year across all tasks is about 0.035 hours.[4]

Table 6-5. Benefits from More Efficient Provisioning by Network and Systems Administrators, per Employee

Activity	Time with ACLs	Time with RBAC	RBAC Savings (minutes)	Times per Employee, per Year	Network Administrator Time Saved per Employee, per Year (hours)	Value per Employee per Year (2009)[a]	Value for a Firm with 10,000 Employees (2009)[a]
Assigning existing privileges to new users	12.4	6.9	5.4	0.20	0.018	$1.22	$12,200
Changing existing users' privileges	7.8	6.6	1.3	0.21	0.004	$0.30	$3,000
Establishing new privileges to existing users	9.2	8.0	1.2	0.20	0.004	$0.28	$2,800
Terminating privileges	7.6	4.7	3.0	0.17	0.009	$0.58	$5,800
Total					**0.035**	**$2.38**	**$23,800**

[a] Value is for 2009 using the 2009 cross-industry national average loaded hourly wage for network and systems administrators ($68.20). Note: All dollar values have been adjusted to real 2009 dollars using the GDP implicit price deflator (BEA, 2009).

[3] Table 6-9 presents the time series of economic benefits from more efficient provisioning. To simplify presentation, time series data are presented once at the end of this chapter in Section 6.10.

[4] For any given organization, the number of times individual tasks occur per year is highly correlated with the number of employees. The data in Table 6-4 are cross-industry averages. Employee turnover was generally comparable across all the industries included in the economic analysis (see Section 5.5), with one exception. The retail industry exhibited significantly higher rates of employee turnover.

The wage rate used to monetize productivity benefits for IT groups was the national fully loaded, mean hourly wage rate for network and systems administrations, denominated in real dollars (2009$). To monetize these savings, simply multiply the[5]

- number of employees (10,000 for 2009),
- amount of time saved per employee (0.035 hours of administrator time), and
- average fully loaded hourly wage rate for an administrator ($68.20 in 2009; BLS, 2010).[6]

For 2009, about 18 million users had at least some of their permissions managed via roles, which generated $37.7 million in economic benefits from higher IT group productivity. See also Appendix B.

6.3 Quantified Benefits from Reduced Employee Downtime from More Efficient Provisioning

Roles significantly reduced the amount of time for which employees were underentitled and thus unable to perform all their job functions. The difference in new employee downtime between using ACLs and roles ranged from no difference to 64 hours, with an average of 6.6 hours across all respondents.

Although employees may not be able to perform all of their job functions without all of their necessary permissions, they are still capable of some level of productivity. In the 2002 study, employees were estimated to be 85% productive while awaiting their permissions. The current survey, however, estimates that employees are only 58% productive without their permissions. This difference in values could reflect the growing reliance of employees on information technology to perform their job functions and further illustrates the value of timely provisioning.

Applying the 6.6 hours of time saved using roles and the 58% productivity level while underentitled, we estimate that the use of roles saves 2.8 hours per employee per time when existing permissions are assigned to new users (Table 6-6). To monetize these 2.8 hours, we used the sector-specific fully loaded hourly wage rate.

Given that the average loaded hourly wage rate in the finance industry was $54.62, a large firm in the finance sector with 10,000 employees would be expected to save $298,000 in productivity gains in 2009 through faster turnaround of permissions. The total economic benefit

[5] This hypothetical example assumes that all users' permissions are managed using roles. In the analysis producing cost-benefit results, an additional layer of complexity was added: the proportion of user permissions managed using roles and the proportion not managed using roles.

[6] This was estimated using the mean wage for a network and computer systems administrator as reported by the BLS. This mean wage was then multiplied by 2.0 to estimate the total cost of employment, including employee benefits, as well as administrative and overhead costs.

Table 6-6. Benefits from Reduction in New Employee Downtime from More Efficient Provisioning, per Employee

Metric	Change in Average Employee Downtime	Productivity Loss Percentage	Equivalent Employee Hours Lost	New Users per Employee	Hours Gained per Employee	Value for a Firm with 10,000 Employees (2009)[a]
Value	6.56	42.07	2.76	0.20	0.55	$298,000

[a] Value in this example is for 2009 using the 2009 average loaded hourly wage for the finance and insurance sector ($54.62). The time series of economic benefits reflects industry-specific wage rates. Note: All dollar values have been adjusted to real 2009 dollars using the GDP implicit price deflator (BEA, 2009).

of reducing new employee downtime was $379.2 million in 2009. See also Tables 5-3 and 5-4 in Chapter 5.

6.4 Quantified Benefits from More Efficient Access Control Policy Maintenance and Certification

The discussion of quantified economic benefits thus far has focused on those that related to provisioning: benefits from reducing the cost of provisioning activities by network and systems administrators and benefits from reducing the amount of time users are underentitled. But there are broader benefits to consider, including enhanced insight into an organization's access control policy and more efficient maintenance of that policy. The task of reviewing policies and maintaining the desired level of consistency across an organization's systems, functions, and groups requires close coordination between managers that engineer and maintain the IT infrastructure and the managers responsible for the business activities that use that infrastructure as a resource for doing their work.

Over 80% of survey respondents reported that roles have improved the efficiency of maintaining their organization's access control policy. One respondent reported the primary business driver for RBAC adoption was "to relate the granting of access to business roles which can be understood by authorizers, as opposed to function permissions, such as the mainframe transaction name, which are not understood by business managers."

Not surprisingly, given the business and security drivers, comments such as this point to how access control policy maintenance is a costly necessity involving several full-time equivalents (FTEs) from both the IT and business divisions of an organization. Roles save IT managers about 0.72 hours per employee, per year and business managers about 0.46 hours per employee per year (Table 6-7). Time savings for business managers were multiplied by the fully loaded mean hourly wage rate for management occupations. Time savings for IT divisions were the average of fully loaded hourly rates for computer systems managers and network administrators to reflect the distribution of IT labor performing access control policy maintenance and certification activities.

Table 6-7. Access Control Policy Maintenance Benefits, per Employee

Category	Time with ACLs per Employee (hours)	Time with RBAC per Employee (hours)	RBAC Savings per Employee (hours)	Loaded Hourly Wage Rate (2009)[a]	Value per Employee (2009)[a]	Value for a Firm with 10,000 Employees (2009)[a]
IT labor	2.39	1.67	0.72	92.10	65.95	695,500
Business labor	1.52	1.07	0.46	98.94	44.79	447,900
Total	**3.91**	**2.74**	**1.19**		**$110.74**	**$1,107,400**

[a] For business labor, the value is for 2009 using the 2009 cross-industry average loaded hourly wage for management occupations. For IT labor, the value is the average for network systems administrators ($68.20) and computer systems managers ($116.00). Note: All dollar values have been adjusted to real 2009 dollars using the GDP implicit price deflator (BEA, 2009).

Although roles do not eliminate the policy review and attestation process, they do make it easier to accomplish, especially when large numbers of employees fall within well-defined job functions for which roles are a particularly effective and efficient access control mechanism. We estimated that RBAC saved $1.8 billion in 2009 from more efficient access control policy maintenance.

A major driver for RBAC adoption has been the regulations described in Chapter 3 that require organizations to certify their access control policies. Organizations perform 1.6 certifications per year, and 136.0 hours of system administrator time is saved per certification when roles are used rather than ACLs. We did not find a significant difference between the amount of time business managers spend per certification when roles are used and when ACLs are used; however, the savings for IT managers were significant.

Applying the fully loaded system administrator hourly wage, we estimate that a typical organization saved about $19,000 per year when using roles to certify their information systems. Unlike the other benefit categories, this benefit was more strongly correlated to the presence of regulation and independent of firm size. Thus, to extrapolate certification benefits, we conservatively assume that these savings accrue only to public companies starting in 2003, the year in which the Sarbanes-Oxley Act went into effect.

Given that there were almost 4,000 public firms in 2009, and 41% were estimated to be using RBAC, we conservatively estimate that RBAC saved about $38 million for that year alone.

6.5 Quantified Costs of RBAC Adoption and Implementation

The most significant expense was role engineering and mapping of permissions and users to roles. Survey results about the costs of implementing RBAC varied significantly, with some organizations spending millions of dollars on custom systems, initiatives related to large-scale ERP implementations, and extensive systems integration services. In contrast, other organizations made use of native role capabilities within systems they were currently using, such as Active Directory and IBM's Resource Access Control Facility (RACF). These organizations

reported spending little to nothing on additional software and services but assigned IT staff to lead and implement the effort.

To understand the costs of implementation, the survey included questions regarding expenditures on hardware, software, and third-party systems integration, services, and role engineering, as well as the level of effort for IT and business groups.[7] To be included in our survey, expenditures were required to be unique to roles to avoid overestimating adoption costs. The typical time required for implementation averaged about 18 months.

As Table 6-8 shows, on average, organizations with more than 500 employees expended $241.01 per employee:

- $201.65 per employee in labor expenditures for IT and business managers to design policies, map permissions and users to roles, and implement the new access control approach,
- $39.36 per employee for one-time nonlabor costs, principally software product expenditures directly related to implementing roles; and
- $1.47 per employee for recurring licensing and maintenance fees to software vendors.

Table 6-8. Average RBAC Implementation Costs, per Employee

Category	Hours per Employee	Loaded Hourly Wage Rate (2009)[a]	Value per Employee (2009)	Average 18-Month Implementation Cost, Firm of 10,000 Employees (2009)
IT labor	0.75	$92.10	$69.37	$693,700
Business labor	1.34	$98.94	$132.28	$1,322,800
Nonlabor costs			$39.36	$393,600
Annual fee			$1.47	$14,700
Total	**2.09**		**$241.01**	**$2,410,000**

[a] For business labor, the value is for 2009 using the 2009 cross-industry average loaded hourly wage for management occupations. For IT labor, the value is the average for network systems administrators ($68.20) and computer systems managers ($116.00). Note: All dollar values have been adjusted to real 2009 dollars using the GDP implicit price deflator (BEA, 2009).

[7] Research, development, and production of software products are among the most labor-intensive processes in the advanced technology sector. Although it is common for economic analyses to account for transfers of value by netting out product-related revenue, the labor intensity associated with developing and customizing RBAC products and product modules for the enterprise computing market is sufficiently high that expenditures on software products were included. We are overestimating the cost basis, but data were insufficient to resolve value added by different tiers in the value chain. Inclusion of these expenditures further reinforces that net economic benefit estimates and public investment performance measures are conservative.

Given that the average adoption and implementation period is 18 months, we assumed that two-thirds of labor costs and all one-time costs were incurred during the first period and that one-third of labor costs and all annual maintenance costs and fees were incurred during the second period.

6.6 Summary Economic Benefits of RBAC, Net of Adoption Costs

Economic benefits before accounting for adoption costs totaled $11 billion between 1994 and 2009.[8] Economic benefits net of adoption costs were $6 billion when accounting for $5 billion in adoption costs (Table 6-9).

All of the benefit categories, however, monotonically increase over time as benefits continue to accrue to all organizations that have adopted RBAC. The stream of benefits net of adoption cost is generally negative prior to the year 2000 and positive afterwards. Although 2009 has the most employees managed using RBAC, there is also a high estimated implementation cost with forecasted accelerated adoption in 2010.

6.7 Net Economic Benefits of RBAC and Net Benefits Attributable to NIST

To estimate net economic benefits attributable to NIST, a counterfactual economic analysis incorporating lower R&D efficiency for software developers and a 1-year delay in RBAC development, and therefore adoption, simulated how net economic benefits would accrue without NIST's involvement. Baseline economic benefits include NIST's impact on R&D efficiency and the timing of RBAC adoption. Software developers' R&D costs were estimated to be $69 million (see Chapter 5), yielding net economic benefits of $6,015 million (Table 6-10).

Delaying RBAC's development by 1 year and increasing the development cost under a scenario in which NIST did not participate in RBAC development has the effect of decreasing net benefits from $6,015 million to $4,905 million, a difference of $1,110 million.

NIST's RBAC activities represented a cost to the government of $2.6 million during the 1990s.[9] Reducing the difference in net economic benefits by $2.6 million in public expenditures yields economic benefits attributable to NIST. We estimate that economic benefits of RBAC attributable to NIST are $1,107 million. Applying the 7% real social discount rate specified by OMB yields an NPV of $835 million (base year = 2000) and a benefit-to-cost ratio of 249.

---

[8] Measured economic benefits are likely conservative because (1) only a subset of industries determined by survey responses, not all industries, was included in the analysis; (2) the minimum firm-size threshold included in the analysis was 500 employees; (3) wage rates used to monetize labor benefits were industry averages for all occupations and included lower-paid occupations that do not necessarily rely on IT for their positions; and (4) only the period of 1994 through 2009 was included in the time series of economic benefits because preceding and later periods could not be estimated accurately; therefore, future benefits of existing implementations were excluded.

[9] Although NIST's researchers were engaged in standardization and research activities after 2000, these costs were not tracked closely because they were incurred on an ad hoc basis and were not considered sufficiently material by NIST management to warrant the expense of formalized reporting.

Table 6-9. Time Series of Economic Benefits of RBAC

Year	Employees Managed Under RBAC (million)	Implementation Costs, ($ millions)	Benefits				Total Economic Benefits ($ millions)	Economic Benefit, Net of Implementation Costs ($ millions)
			More Efficient Provisioning ($ millions)	Reduced Employee Down Time ($ millions)	Access Control Policy Maintenance ($ millions)	Access Control Policy Certification ($ millions)		
1994	0.0	−152.6	0.0	0.0	0.0	0.0	0.0	−152.6
1995	1.0	−111.1	1.1	10.3	46.5	0.0	57.8	−53.3
1996	1.4	−75.3	2.6	27.7	109.3	0.0	139.5	64.2
1997	1.8	−75.6	3.4	34.8	141.9	0.0	180.1	104.5
1998	2.1	−83.9	4.1	42.0	174.4	0.0	220.6	136.6
1999	2.5	−225.5	5.0	48.6	209.3	0.0	262.9	37.4
2000	3.9	−140.4	7.2	68.2	301.4	0.0	376.7	236.3
2001	4.3	−62.8	9.4	87.8	390.9	0.0	488.1	425.2
2002	4.5	−91.2	10.1	103.2	445.7	0.0	559.0	467.8
2003	4.9	−109.3	10.9	111.7	491.8	8.6	623.1	513.8
2004	5.4	−414.8	12.1	120.7	543.2	9.5	685.4	270.6
2005	7.7	−565.9	15.2	150.3	683.0	11.8	860.3	294.3
2006	10.1	−471.0	20.7	205.0	938.6	16.0	1,180.4	709.4
2007	11.9	−420.6	25.9	256.1	1,186.7	20.0	1,488.7	1,068.1
2008	13.6	−894.4	30.1	301.2	1,396.9	23.3	1,751.6	857.2
2009	18.0	−1,094.4	37.7	379.2	1,752.1	29.1	2,198.2	1,103.7
Total		**−4,988.9**	**195.5**	**1,946.6**	**8,811.8**	**118.3**	**11,072.3**	**6,083.4**

Note: Industries were defined by 2-digit NAICS code and included utilities; manufacturing; wholesale trade; retail trade; information; finance and insurance; professional, scientific, and technical services; educational services; health care and social assistance; arts, entertainment, and recreation; other services; and public administration. All dollar values have been adjusted to real 2009 dollars using the GDP implicit price deflator (BEA, 2009).

Table 6-10. Net Economic Benefits of RBAC and Net Benefits Attributable to NIST

	Baseline Net Benefits of RBAC			Net Benefits without NIST				
Year	R&D Expenditures ($ millions)	End-User Benefits ($ millions)	Net Benefits ($ millions)	R&D Expenditures ($ millions)	End-User Benefits[a] ($ millions)	Net Benefits ($ millions)	NIST Expenditures ($ millions)	Net Benefits Attributable to NIST ($ millions)
1992							−0.1	-0.1
1993							−0.1	-0.1
1994		−152.6	−152.6				−0.2	−152.9
1995		−53.3	−53.3		−152.6	−152.6	−0.6	98.7
1996	−6.24	64.2	58.0		−53.3	−53.3	−0.6	110.7
1997	−6.24	104.5	98.2	−6.80	64.2	57.4	−0.5	40.3
1998	−6.24	136.6	130.4	−6.80	104.5	97.7	−0.4	32.3
1999	−6.24	37.4	31.2	−6.80	136.6	129.8		−98.7
2000	−6.24	236.3	230.1	−6.80	37.4	30.6		199.4
2001	−6.24	425.2	419.0	−6.80	236.3	229.5		189.4
2002	−6.24	467.8	461.6	−6.80	425.2	418.4		43.2
2003	−6.24	513.8	507.6	−6.80	467.8	461.0		46.5
2004	−6.24	270.6	264.3	−6.80	513.8	507.0		−242.7
2005	−6.24	294.3	288.1	−6.80	270.6	263.8		24.3
2006	−6.24	709.4	703.2	−6.80	294.3	287.5		415.7
2007		1,068.1	1,068.1	−6.80	709.4	702.6		365.5
2008		857.2	857.2		1,068.1	1,068.1		−210.9
2009		1,103.7	1,103.7		857.2	857.2		246.5
Total	**−68.7**	**6,083.4**	**6,014.7**	**−74.8**	**4,979.6**	**4,904.8**	**−2.6**	**1,107.3**
	NPV of net benefits ($ millions, base year = 2000)							8,350
	Benefit-to-cost ratio							249

Note: All dollar values have been adjusted to real 2009 dollars using the GDP implicit price deflator (BEA, 2009).

7. SUMMARY RESULTS AND CONCLUDING REMARKS

This analysis quantified net economic impacts of RBAC totaling more than $6 billion between 1992 and 2009 (Table 7-1). Total cost savings were estimated at $11 billion, but these were offset by $5 billion in adoption costs and a mere $69 million in development costs.

For 1995 we estimated just under a 4% penetration rate for employees, growing to about 11% in 2002, 13% in 2004, and 41% in 2009. We defined the penetration rate over time to be the proportion of employees at organizations with a staff of 500 or more with at least some of their permissions managed using roles.

NIST offered the first formal description of RBAC in 1992, later collaborating with Ravi Sandhu to develop the comprehensive RBAC model and standard that would be accepted as ANSI/INCITS standard 359-2004. Software developers and systems integrators noted that NIST not only accelerated RBAC's introduction into software products, but it also reduced their development costs. NIST's development of generic RBAC technology and infratechnology supported the emergence of a broad ecosystem of software products, systems integration services, and consulting services.

For the relatively small sum of $2.6 million, society accrued at least $1.1 billion in benefits between 1992 and 2009 that are directly attributable to NIST (Table 7-1). With a base year of 2000, the base year used in the 2002 study, the NPV is $835 million when the OMB-specified 7% real social discount rate is applied. The benefit-to-cost ratio is 249, meaning that society accrued $249 in economic benefits for every $1 NIST invested in RBAC initiatives.

NIST's RBAC project was the product of an assessment conducted by NIST research staff in 1992 (Ferraiolo, Gilbert, and Lynch, 1992) that was itself catalyzed by industry requests for a security solution suited to commercial/industrial requirements in the 1980s and early 1990s. The industry needs assessment indicated a clear role and rationale for NIST, catalyzing the investment by NIST and NSA of a relatively small sum ($2.6 million in 2009 dollars) to provide the resources needed to devise a solution to industry needs, offer a formal RBAC specification, develop proof-of-concept implementations, investigate and publish research results, and lead an effort for ANSI/INCITS standardization.

Table 7-1. Summary Measures of Economic Return, 1992–2009

	Baseline Economic Analysis (with NIST)	Counterfactual Economic Analysis (without NIST)	Attribution to NIST
Total economic benefits before adoption costs ($ millions)	11,072.3	8,874.1	
End user adoption costs ($ millions)	−4,988.9	−3,894.5	
Economic benefits net of adoption costs ($ millions)	6,083.4	4,979.6	
RBAC development costs ($ millions)	-68.7	−74.8	−2.6
Net economic benefits ($ millions)	6,014.7	4,904.8	1,109.8
Net economic benefits attributable to NIST			1,107.3
NPV of net benefits ($ millions, base year = 2000)			835.0
Benefit-to-cost ratio			249

Note: All dollar values have been adjusted to real 2009 dollars using the GDP implicit price deflator (BEA, 2009). Impacts were calculated for organizations with 500 or more employees in the following industries defined by 2-digit NAICS code: utilities; manufacturing; wholesale trade; retail trade; information; finance and insurance; professional, scientific, and technical services; educational services; health care and social assistance; arts, entertainment, and recreation; other services; and public administration.

7.1 Comparison between the 2002 Prospective and 2010 Retrospective Economic Analyses

The 2010 study afforded the opportunity to revisit 2002's prospective economic analysis, which relied on forecasts of adoption and benefits, and compare these results with those from a retrospective analysis. While the primary drivers behind the 2010 study were to assess RBAC's economic benefits and report on the state of RBAC adoption, it was also undertaken to provide researchers with a lens into how comparative assessments might be conducted.

The 2002 study was a valuable resource in that the research staff was familiar with the technology, categories of economic cost and benefit for end users and software developers were known, and NIST's role in accelerating RBAC development was well documented. Yet overreliance on the earlier study had the potential to introduce bias into the research process by training researchers to recognize and focus on previously identified impact categories. To limit the degree to which it predisposed the research staff to following only known lines of inquiry, early in the research process the 2002 study was inventoried and then purposefully set aside. We cataloged its technical impact measurements and estimated parameters (i.e., turnover ratios, productivity ratios, time measurements, labor-hour savings) for benefit and cost categories but ignored adoption rates, economic impact metrics (i.e., wages and other dollar-denominated values) (Table 7-2).

Table 7-2. Differences in Approach and Adjustments for Comparison, 2002 and 2010 Studies

Benefit-Cost Category	2002 Study	2010 Study	Adjustment for Comparative Assessment, if Any
Quantified end user benefits and costs			
More efficient provisioning by network and systems administrators	***Included***	***Included***	
Labor savings measurement	Time savings in minutes for 4 common provisioning activities (Table 7-4)	Retained estimates from 2002	Estimates from 2002 were representative of benefits of RBAC; values measured in 2010 likely would have reflected other technology development in addition to RBAC
Turnover ratios	2002 estimates (Table 7-3)	2010 estimates (Table 7-3)	
Labor cost measurement	National mean hourly wage for network and systems administrators for 1999 (2000$)	National mean hourly wage for network and systems administrators by year (2009$)	Updated 2002 study's model to reflect actual historical wage data by industry
Reduction in new employee downtime from more efficient provisioning	***Included***	***Included***	
Labor savings measurement	2002 estimate of reduction in time to permissions (Table 7-3)	2010 estimate of reduction in time to permissions (Table 7-3)	
Productivity loss	2002 estimate (Table 7-3)	2010 estimate (Table 7-3)	
Labor cost measurement	National mean hourly wage for white-collar employees for 1999 (2000$)	National mean hourly wage for all occupations, by industry and year (2009$)	Updated 2002 study's model to reflect actual historical wage data by industry; the time series used in the 2002 is no longer maintained by BLS
More Efficient Access Control Policy Maintenance and Certification	***Not included***	***Included***	Updated 2002 model to reflect the presence of this benefit during study time frame
Labor savings measurement (maintenance)		Incremental hours required to maintain and assess access control policy and controls using roles vs. not using roles (IT and business operations staff)	
Labor cost measurement (maintenance)		Average of national mean hourly wage for network and systems administrators and by year (2009$) and national mean hourly wage for management occupations by year (2009$)	
Labor savings measurement (certification)		Incremental hours required to maintain and assess access control policy and controls using roles vs. not using roles (network and systems administrators and business managers)	

(continued)

Table 7-2. Differences in Approach and Adjustments for Comparison, 2002 and 2010 Studies (continued)

Benefit-Cost Category	2002 Study	2010 Study	Adjustment for Comparative Assessment, if Any
Turnover ratio (certification)		Mean estimated number of certifications conducted per year	
Labor cost measurement (certification)		National mean hourly wage for network and systems administrators by year (2009$) and national mean hourly wage for management occupations by year (2009$)	
RBAC adoption costs			
Labor effort	Labor hours for network and systems administrators and business managers	Labor hours for network and systems administrators and business managers	
Labor cost measurement	National mean hourly wage for network and systems administrators by year (2000$)	National mean hourly wage for network and systems administrators by year (2009$) and national mean hourly wage for management occupations by year (2009$)	
Non-labor expenditures	Services, software programming, and maintenance fees	Services, software programming, and maintenance fees	
Adoption time	12 months	18 months	
Software Developer Costs	Estimated software development costs associated with incorporating RBAC functionality	Estimated software development costs associated with incorporating RBAC functionality	Adjusted to 2009$
NIST's Expenditures	Actual NIST expenditures	Actual NIST expenditures	Adjusted to 2009$
Time period of analysis	R&D Costs: 1992-2005 Benefits: 2000-2006	Costs: 1992-2005 Benefits: 1992-2009	Compared through 2006.
Industries	Information; finance and insurance; healthcare and social assistance; professional, technical, and scientific services; manufacturing; utilities; transportation and warehousing	Information; finance and insurance; healthcare and social assistance; professional, technical, and scientific services; manufacturing; utilities; transportation and warehousing; wholesale trade; retail trade; educational services; arts, entertainment, and recreation; and public administration	Compared actual results as well as with common industries only
Unit-scaling factor	Employment in for firms >500 employees for 2000 was assumed to be held constant for 2000 to 2006; only rate of adoption was varied.	Actual employment in for firms >500 employees.	Updated 2002 study's model to reflect actual employment data by industry by year; harmonized industries

In 2010, most commercially available enterprise software products were either compatible with RBAC or had embedded role capabilities. Unlike the 2002 study, in which many products had yet to be engineered to enable sufficiently granular access control for use with RBAC, the current issue is not so much whether role capabilities were available, but rather how to take advantage of them. In other words, many of the same adoption challenges identified in the 2002 study—role engineering, size of investment, legacy systems, and interoperability—persisted in

2010. These findings were confirmed through reviews of the scholarly and grey literature, which showed that new work in the field focused on narrow, specific issues in RBAC, such as RBAC and attributes, as opposed to broader topics, such as implementation or role engineering.

The literature in particular proved to be most useful because it documented use-cases for RBAC in access control policy maintenance, audit, and certification. This category proved to be the most significant source of economic benefit, yet it was treated only qualitatively in the 2002 study. The reason for this was because key regulatory drivers for financial corporations, publicly traded companies, and other heavily regulated industries had not yet been enacted or were just taking effect. For instance, Sarbanes-Oxley's internal controls, internal control audit, and certification requirements were enacted in 2002, after the first study was published. In 2010, ARRA enhanced the privacy provisions of HIPAA and now requires health care organizations to disclose any breaches in personal health information.

Interviews with experts therefore had as their primary focus

- review of current trends in best practice in IAM and technology and standards development;
- review and comparison of their perceptions of actual adoption, costs, and benefits to those forecast by RTI in 2002;
- exploration of emerging categories of economic benefit and cost, such as access control policy maintenance; and
- discussion of persistent challenges and needs.

During these discussions, which occurred over the course of a year and often involved multiple discussions with the same experts, we learned that of all the technical impact measurements, the one for the time savings per task was the one that was most valid and still held (Table 7-3).

IAM systems have improved significantly over the past few years, and often these benefits are not directly related to RBAC. Attempting to reestimate the time savings of conducting four common provisioning tasks would likely yield inaccurate results because substantial innovation has yielded self-service tools as well as greater automation.

Although we retained the original time-savings estimates, we updated the estimates for labor productivity when under entitled and the frequency with which common provisioning tasks occur. These technical impact metrics are independent of the time savings associated with roles and speak more to the use of and efficiency gains from IT in the workplace and trends in user life-cycle management, respectively. Indeed, the 2002 study relied upon consensus expert opinion and set the model to assume that users are approximately 85% as productive when underentitled as with their permissions. This study actually measured that productivity loss to be 42%.

Table 7-3. Technical Impact Unit Estimates, 2002 and 2010 Studies

	2002 Study	2010 Study
More efficient provisioning (time savings per task in minutes)		
Frequency of assigning existing permissions to new users	5.5 min	5.5 min
Frequency of changing existing users' permissions	1.2 min	1.2 min
Frequency of establishing new permissions for existing users	1.2 min	1.2 min
Frequency of terminating permissions	2.9 min	2.9 min
More efficient provisioning (per year, per employee)		
Frequency of assigning existing permissions to new users	1.3 times/emp	0.20 times/emp
Frequency of changing existing users' permissions	1.5 times/emp	0.21 times/emp
Frequency of establishing new permissions for existing users	1.06 times/emp	0.21 times/emp
Frequency of terminating permissions	0.22 times/emp	0.17 times/emp
Reduction in new employee downtime		
Incremental time period during which user is underentitled		
Productivity loss while user is underentitled	15%	42%
Adoption time	12 months	18 months

The 2010 study also makes adjustments to changes in the underlying data series, not simply extrapolating historical trends. The 2002 study relied on BLS's national mean hourly wage rate for white-collar workers to monetize economic impacts denominated in hours. That series was retired by the Census, and in its place mean wage rates by industry were used.

The effect of this change is visible in Table 7-4 when comparing the economic benefits per employee, per year for 2006:

- reported in 2002 was a benefit of $44.03 per employee, in 2000 dollars;
- adjusted to 2009 dollars using the GDP implicit price deflator, but before refreshing underlying wage rates from BLS, the benefit is equivalent to $54.45 per employee; and
- adjusted to 2009 dollars and using refreshed underlying wage data, the benefit is $51.97 per employee, even though the all technical impact measurements are exactly the same.

The survey for the 2002 study was fielded with the assistance of Information Security magazine. Information Security sent e-mails to its listserv introducing the study and requesting participation. In years since that survey was fielded, and in response to privacy concerns and the sale and resale of e-mail distribution lists, these avenues for distributing survey links have declined in effectiveness. Therefore, a different strategy was used. We fielded our survey

Table 7-4. Economic Impact Unit Estimates for 2006, 2002 and 2010 Studies

	2002 Study per Employee, per Year (2000$)	2002 Study per Employee, per Year (2009$), *before* Adjustment to Actuals	2002 Study per Employee, per Year (2009$), *after* Adjustment to Actuals	2010 Study per Employee, per Year (2006 only)
More efficient provisioning	$9.40	$11.63	$12.13	$2.33
Reduction in new employee downtime	$34.63	$42.82	$39.84	$23.04
Access control policy maintenance and certification	NA	NA	$90.18	$90.18
End user adoption costs	$78.36	$96.89	$96.89	$241.01

instrument through conference notifications, social media, and e-mail distribution lists sponsored by professional and trade associations and IT research groups. Reaching respondents through only one distribution channel presented an unacceptable level of risk.

7.2 Comparison of Forecasted and Actual RBAC Adoption

The 2002 study relied on expert input to estimate a range of sector-specific estimates of prospective adoption in 2006. This was necessary because little information was available about end user adoption; most information was anecdotal and the Internet survey measured very low levels of adoption relative to expected future use. Adoption between 2001 and 2005 was estimated by applying points on an S-shaped adoption curve to these 2006 estimates. The basis for extrapolating to national impact estimates was total employment for 2000, which was assumed to be representative of 2001 through 2006 (Table 7-5). Accordingly, net economic benefits were expressed as a range based on survey responses and expert opinion: low, medium, and high penetration scenarios.

Not only did the 2010 study estimate adoption for the same period as the 2002 study, but it collected empirical evidence for adoption between 1995 and 2000 and also 2007 through the middle of 2010. Although the 2002 attempted to capture pre-2000 adoption, it was unable to because RBAC was in the earliest stages of its technology life cycle and reliable information on adoption was unavailable. The 2010 study overcame that limitation through data collection and interviews with earlier adopters.

The top portion of Figure 7-1 presents the estimated number of employees with at least some permissions managed by RBAC. Note that the actual adoption, when measured in millions of employees, between 2003 and 2006 was within range predicted by experts. Because the industries included in each study differed, we also offer a comparison of the estimated

Table 7-5. Difference in Employment Base for Extrapolation of Cost-Benefit Results, 2002 and 2010 Studies

Year	2002 Study Employment Base	2010 Study Employment Base	Comments
1995		40,714,035	Employment in organizations with more than 500 employees was not a data series until 1998; Data for 1998 were assumed to be representative
1996		40,714,035	
1997		40,714,035	
1998		40,714,035	
1999		41,550,244	
2000	31,597,019	42,276,837	In the 2002 study employment data for 2000 was assumed to be representative for 2001 to 2006. RBAC penetration varied along an s-curve of technology adoption to simulate the proportion of forecasted adoption over time
2001	31,597,019	42,980,616	
2002	31,597,019	42,048,622	
2003	31,597,019	42,384,693	
2004	31,597,019	42,776,374	
2005	31,597,019	43,010,883	
2006	31,597,019	44,000,596	
2007		44,469,890	
2008		44,469,890	Data for 2008 and 2009 were unavailable; data for 2007 were assumed to be representative
2009		44,469,890	

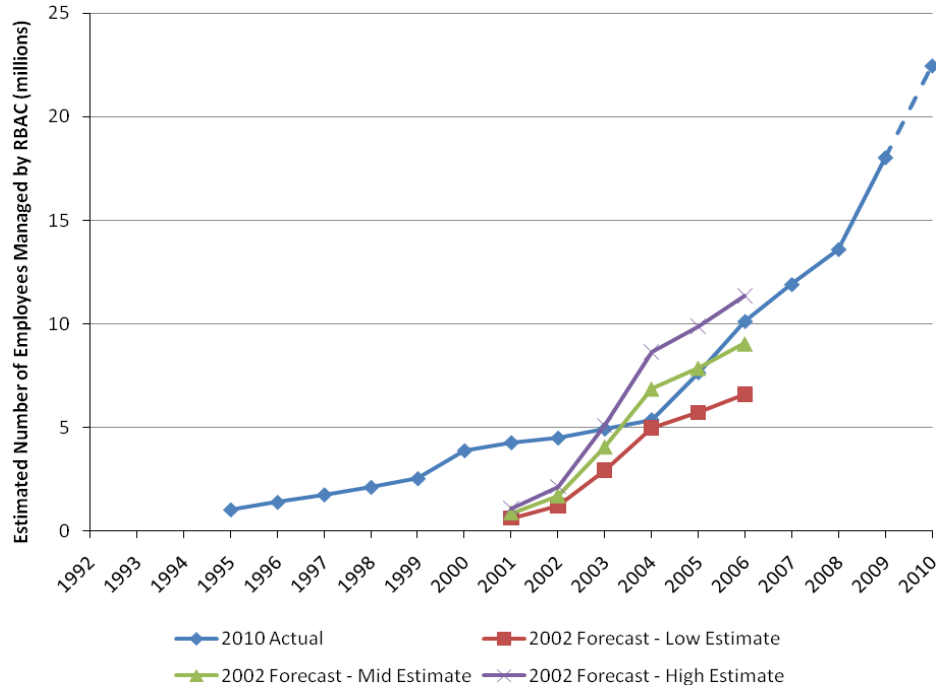
penetration rate, depicted in the lower half of Figure 7-1. Here, we learn that actual penetration was within the range predicted by the 2002 study between 2003 and 2006. Penetration in 2006 was within the band defined by the 2002 study's mid and high estimate.

7.3 Comparison of Forecasted and Actual Net Economic Benefits

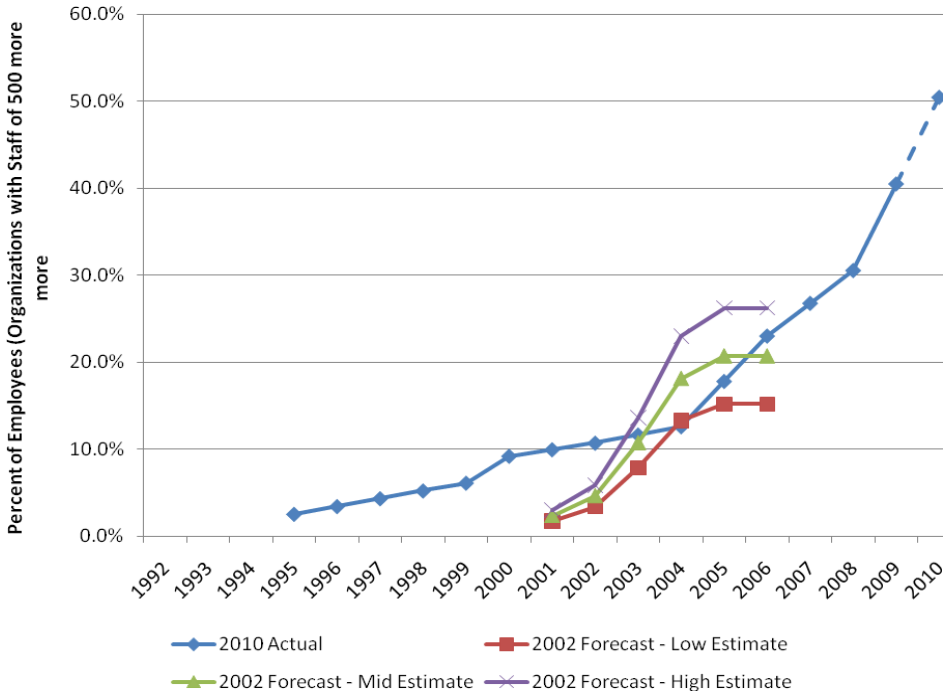
Table 7-6 details the results from the 2002 study, before any adjustments. In real 2000 dollars, the study projected net economic benefits of RBAC (Midpoint Estimate) to be $895 million for 1992 through 2006. Net benefits attributable to NIST were projected to be $377.4 million. In comparison, this study projected net economic benefits between 1992 and 2009 to be $6,015 million, with $1,107 million attributable to NIST.

Given the differences in estimation methodologies between the 2002 and 2010 study, adjustments were made to bring the studies into alignment to enable fair comparison. The 2002 model was refreshed to use the same actual employment and sector-specific wages used in the 2010 study and was expanded to include the access control policy maintenance category. The 2010 study was modified to include only those sectors included in the 2002 study, no certification benefits per business, and stopping the benefit estimation in 2006 (with no

Figure 7-1. Comparison of Forecasted and Actual RBAC Adoption, 1992–2010



Adoption (Millions of Employees)



Adoption (Percentage of Employees)

Table 7-6. The 2002 Study's Net Economic Benefits Attributable to NIST (Midpoint Estimate)

	Baseline Net Benefits of RBAC			Net Benefits without NIST				
Year	R&D Expenditures ($ millions, 2000$)	End-User Benefits ($ millions, 2000$)	Net Benefits ($ millions, 2000$)	R&D Expenditures ($ millions, 2000$)	End-User Benefits ($ millions, 2000$)	Net Benefits ($ millions, 2000$)	NIST Expenditures ($ millions, 2000$)	Net Benefits Attributable to NIST ($ millions, 2000$)
1992	—	—	—	—	—	—	0.06	—
1993	—	—	—	—	—	—	0.06	—
1994	—	—	—	—	—	—	0.19	—
1995	—	—	—	—	—	—	0.47	—
1996	−5.05	—	−5.05	—	—	—	0.45	−5.05
1997	−5.05	—	−5.05	−5.50	—	−5.50	0.39	0.45
1998	−5.05	—	−5.05	−5.50	—	−5.50	0.34	0.45
1999	−5.05	—	−5.05	−5.50	—	−5.50	0.04	0.45
2000	−5.05	−13.03	−18.08	−5.50	—	−5.50	0.04	−12.58
2001	−5.05	4.69	−0.36	−5.50	−11.40	−16.90	0.04	16.54
2002	−5.05	24.89	19.84	−5.50	5.17	−0.33	—	20.17
2003	−5.05	65.31	60.26	−5.50	24.04	18.54	—	41.72
2004	−5.05	212.13	207.08	−5.50	61.82	56.32	—	150.76
2005	−5.05	313.56	308.51	−5.50	199.03	193.53	—	114.97
2006	—	337.85	337.85	−5.50	293.83	288.33	—	49.52
Total	**−50.50**	**945.40**	**894.90**	**−55.00**	**572.49**	**517.49**	**2.08**	**377.40**

Source: Gallaher et al., 2002.

additional adoption assumed for 2007). Thus, although penetration rates and economic impact metrics reflected each study's estimates, the time period of analysis, impact categories, and underlying data series for wages and employment were the same.

Overall, the 2010 metrics yield a total of $3.0 billion in benefits (Table 7-7), while the 2002 metrics yield $3.9 billion (Table 7-8). The 2010 metrics provide a longer time series for benefits to accrue; however, we now estimate higher implementation costs and longer implementation time (1.5 vs. 1 year) in the 2010 study. In addition, the 2010 metrics for productivity result in 62% less productivity benefits than those measured in the 2002 study. In retrospect, the 2002 study may have overestimated the ratio of new users to employees: 1.3 to 0.2 for the 2010 study. This is not necessarily an error because it is possible that single sign-on and other approaches have greatly reduced the number of user accounts held by the average employee.

Table 7-7. 2010 Model—Adjusted for Comparison

Year	Employees (thousands)	Implementation and Adoption Costs ($ millions)	More Efficient Provisioning ($ millions)	Reduced Employee Down Time ($ millions)	Access Control Policy Maintenance ($ millions)	End-User Benefits, Net of Implementation Costs ($ millions)
1994		−120	—	0	—	−120
1995	817	−88	1	9	37	−41
1996	1,103	−59	2	24	86	53
1997	1,389	-60	3	30	112	85
1998	1,675	−66	3	36	138	111
1999	1,999	−176	4	42	165	34
2000	3,055	−109	6	59	237	192
2001	3,354	−46	7	75	307	344
2002	3,507	−79	8	87	348	365
2003	3,902	−82	9	95	386	408
2004	4,209	−317	9	103	427	222
2005	5,957	−434	12	128	532	238
2006	7,846	−132	16	174	728	786
Total		**−1,767**	**80**	**860**	**3,502**	**2,675**

Note: All dollar values have been adjusted to real 2009 dollars using the GDP implicit price deflator (BEA, 2009).

Setting aside these adjustments, one can simply review the predicted and actual measures of economic return (Table 7-9). The 2002 study predicted the NPV of net benefits attributable to NIST to be $226 million to $525 million (2009$, base year = 2000), the BCR to be 69 to 158, and the IRR to be 39% to 90%.

The NPV for the 2010 study was $835 million (2009$, base year = 2000) and the BCR was 249. The IRR on the time series of net benefits attributable to NIST in the 2010 study could not be calculated because of intermittent negative cash flows.

Clearly, NIST's RBAC activities exceeded expectations given that the BCR calculated retrospectively was 249 (1992-2009), greatly exceeding the upper-bound estimate of 158 calculated in 2002. Notably, even if the retrospective BCR was limited to years through 2006 only, it would still be 203. Similarly, if the 2010's NPV is set to through 2006 only, it would be $596 million, which is only $70 million more than the NPV for the high estimate of $525 million.

Table 7-8. 2002 Model—Adjusted for Comparison

Year	Employees (thousands)	Implementation and Adoption Costs ($ millions)	More Efficient Provisioning ($ millions)	Reduced Employee Down Time ($ millions)	Access Control Policy Maintenance ($ millions)	End-User Benefits, Net of Implementation Costs ($ millions)
1994	—	—	—	—	—	—
1995	—	—	—	—	—	—
1996	—	—	—	—	—	—
1997	—	—	—	—	—	—
1998	—	—	—	—	—	—
1999	—	—	—	—	—	—
2000	—	−84	—	—	—	−84
2001	870	−81	10	33	83	46
2002	1,705	−228	20	69	173	34
2003	4,060	−272	49	164	423	364
2004	6,867	−97	84	275	722	984
2005	7,866	−115	95	312	823	1,115
2006	9,055	0	110	361	956	1,426
Total		**−877**	**369**	**1,214**	**3,181**	**3,886**

Note: All dollar values have been adjusted to real 2009 dollars using the GDP implicit price deflator (BEA, 2009).

Table 7-9. Comparison of Measures of Economic Return

Measure of Economic Return	Results from 2002 Prospective Economic Analysis			Results from 2010 Retrospective Economic Analysis
	Low	Mid	High	
Net Present Value ($ million, base year = 2000)[a]	226.3	361.1	525.5	835.0
Benefit-to-Cost Ratio	69	109	158	249[b]
Internal Rate of Return	39%	62%	90%	—

[a] Although the base year is 2000, the dollar values have been adjusted to 2009 terms to match those. In 2000 dollars, the NPV for the 2002 study ranged from $183 million to $425 million.

[b] If net benefits attributable to NIST were restricted to only those accruing from 1992 to 2006, to match the 2002 study's estimate, the BCR would be 203 and the NPV would be $596 million.

REFERENCES

Anderson, A. 2004. XACML Profile for Role Based Access Control (RBAC). <http://docs.oasis-open.org/xacml/cd-xacml-rbac-profile-01.pdf>.

Anderson, R.J. 2001. *Security Engineering: A Guide to Building Dependable Distributed Systems*. New York: Wiley Computer Publishing.

Barkley, J.F. (no date). "Workflow Management Employing Role-Based Access Control." U.S. Patent #6,088,679.

Barkley, J.F. 1995a. "Application Engineering in Health Care." Second Annual CHIN Summit. Chicago, IL. <http://www.itl.nist.gov/div897/staff/barkley/proj/paper.pdf>.

Barkley, J.F. 1995b. "Implementing Role-based Access Control Using Object Technology." First ACM Workshop on Role-Based Access Control.

Barkley, J.F., and A.V. Cincotta. 1998. "Managing Role/Permission Relationships Using Object Access Types." Third ACM Workshop on Role-Based Access Control, Fairfax, VA.

Barkley, J.F., and A.V. Cincotta. 2001. "Implementation of Role/Group Permission Association Using Object Access Type." U.S. Patent No. 6,202,066.

Barkley, J.F., A.V. Cincotta, D.F. Ferraiolo, S. Gavrila, and D.R. Kuhn. 1997. "Role-based Access Control for the World Wide Web." 20th National Computer Security Conference.

Barkley, J.F., D.R. Kuhn, Rosenthal, Skall, and A.V. Cincotta. 1998. "Role-Based Access Control for the Web." CALS Expo International & 21st Century Commerce 1998: Global Business Solutions for the New Millennium.

Bednarz, J. 2005. "Compliance: Thinking Outside the Sarbox." *Network World*. As obtained on 10/31/2008 at http://www.networkworld.com/research/2005/020705sox.html.

Bertino, E. and R. Sandhu. 2005. "Database Security—Concepts, Approaches, and Challenges." IEEE Transactions on Dependable and Secure Computing 2(1): 2-19.

Bokhari, Z. 2009. Standard & Poor's Industry Surveys, Computers: Software. (April 23) and company Web sites. U.S. Code 44 (2006). Information Security, § 3532 (b) (1). <http://www.gpoaccess.gov/uscode/index.html>. Accessed February 5, 2009.

Bureau of Economic Analysis. 2009. "National Income and Product Accounts: Table 5.3.5. Private Fixed Investment by Type." <http://www.bea.gov/national/nipaweb/Index.asp>. Accessed April 14, 2009.

Byrnes, C., Vice-President: Services and Systems Management, The META Group. June 13, 1997. "Security Administration Grows Up." An analyst report produced for Tivoli, an IBM company.

Chandramouli, R. and R. Sandhu. 1998. "Role-based Access Control Features in Commercial Database Management Systems." 21st National Information Security Conference.

Coyne, E.J., and J.M. Davis. 2007. *Role Engineering*. Norwood, MA: Artech Publishing.

Coyne, E., and T. Weil. 2008. "An RBAC Implementation and Interoperability Standard: The INCITS Cyber Security 1.1 Model." *IEEE Security and Privacy* 6(1):84-87.

Federal Trade Commission. 2002. "16 CFR Part 314: Standards for Safeguarding Customer Information; Final Rule." *Federal Register* 67:100, p. 36483-36494. <http://www.ftc.gov/os/2002/05/67fr36585.pdf>.

Ferraiolo, D., and J. Barkley. 1997. "Specifying and Managing Role-Based Access Control within a Corporate Intranet." In *Proceedings of the Second ACM Workshop on Role-Based Access Control,* 77-82. Fairfax, VA: ACM. doi:10.1145/266741.266761.<http://portal.acm.org/citation.cfm?id=266741.266761>.

Ferraiolo, D.F., J.F. Barkley, and D.R. Kuhn. 1999. "A Role-based Access Control Model and Reference Implementation within a Corporate Intranet." *ACM Transactions on Information Systems Security* 1(2):34-64.

Ferraiolo, D.F., R. Chandramouli, G-J Ahn, and S.I. Gavrila. 2003. "The Role Control Center: Features and Case Studies." In *Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies*, 12-20. Como, Italy: ACM. doi:10.1145/775412.775415. <http://portal.acm.org/citation.cfm?id=775415>.

Ferraiolo, D.F., J.A. Cugini, and R. Kuhn. 1995. "Role-based Access Control: Features and Motivations." In *Proceedings of the Eleventh Annual Computer Security Applications Conference*. New Orleans, LA.

Ferraiolo, D. and S. Gavrila. (pending). "A Method for Visualizing and Managing Role-Based Policies on Identity-Based Systems."

Ferraiolo, D.F., D.M. Gilbert, and N. Lynch. 1992. *Assessing Federal and Commercial Information Security Needs*. NISTIR 4976. Gaithersburg, MD: National Institute of Standards and Technology.

Ferraiolo, D.F., and D.R. Kuhn. 1992. "Role-based Access Control." 15th National Computer Security Conference. NIST/NSA.

Ferraiolo, D.F., D.R. Kuhn, and R. Chandramouli. 2003, revised 2007. *Role-based Access Control.* Norwood, MA: Artech House.

Ferraiolo, D.F., R. Kuhn, and R. Sandhu. 2007. "RBAC Standard Rationale: Comments on a Critique of the ANSI Standard on Role Based Access Control." *IEEE Security & Privacy* 5(6):51-53.

Ferraiolo, D.F., R. Sandhu, S. Gavrila, D.R. Kuhn, and R. Chandramouli. 2001. "Proposed NIST Standard for Role-Based Access Control." *ACM Transactions on Information and System Security* 4(3):224-274.

Gallaher, M., A. O'Connor, and B. Kropp. 2002. *The Economic Impact of Role-Based Access Control*. Prepared for the National Institute of Standards and Technology. Research Triangle Park, NC: RTI International.

Gavrila, S.I., and J. F. Barkley. 1998. "Formal Specification for Role Based Access Control User/Role and Role/Role Relationship Management." In *Proceedings of the third ACM workshop on Role-based access control*, 81-90. Fairfax, Virginia, United States: ACM. doi:10.1145/286884.286902. http://portal.acm.org/citation.cfm?id=286884.286902.

Geroski, P.A. 2000. "Models of Technology Diffusion." *Research Policy* 29:603-655.

Health Care Financing Administration (HCFA). 2001. "General Questions." <http://www.hcfa.gov/extpart/faqs/faq-genqt.htm>. As obtained on June 13, 2001.

Kampman, K., and H. Purdue. 2006. *The Business of Roles*. Midvale, UT: The Burton Group.

Kampman, K. 2007. *Role Management in the Enterprise: Street Scenes*. Midvale, UT: The Burton Group.

Kuhn, D.R. (no date). "Implementation of Role-based Access Control in Multi-level Secure Systems." U.S. Patent No. 6,023,765.

Kuhn, D.R. 1997. "Mutual Exclusion of Roles as Means of Implementing Separation of Duty in Role-Based Access Control Systems." Second ACM Workshop on Role-Based Access Control.

Kuhn, D.R. October 22-23, 1998. *"Role Based Access Control on MLS Systems Without Kernel Changes."* Third ACM Workshop on Role Based Access Control.

Kuhn, D.R., E.J. Coyne, and T.R. Weil. 2010. "Adding Attributes to Role-Based Access Control." *Computer* 43(6):79-81.

Leahu, M., M. Dobson, and G. Avolio. 2008. "Access Control Design and Implementation in the ATLAS Experiment." IEEE Transactions on Nuclear Science 55(1):386-391.

Ledig, R. 2000. "Gramm-Leach-Bliley Act Financial Privacy Provisions: The Federal Government Imposes Broad Requirements to Address Consumer Provacy Concerns." Fried, Frank, Harris, Shriver, & Jacobson. <http://www.ffhsj.com/bancmail/bmarts/edcp_art.htm>. Accessed June 14, 2001.

Mahajan, V., and R.A. Peterson. 1985. "Models for Innovation Diffusion." Sage University Paper Series on Quantitative Applications in the Social Sciences, 07-048. Beverly Hills and London: Sage Publications.

Martin, S.A., D.L. Winfield, A.E. Kenyon, J.R. Farris, M.V. Bala, and T.H. Bingham. 1998. "A Framework for Estimating the National Economic Benefits of ATP Funding of Medical Technologies—Preliminary Applications to Tissue Engineering Projects Funded from 1990 to 1996." Prepared for the National Institute of Standards and Technology. Research Triangle Park, NC: RTI.

Ni, Q, E. Bertino, J. Lobo, and S.B. Calo. 2009. "Privacy-Aware Role-Based Access Control." *Security and Privacy* 7(4):35-43.

National Institute of Standards and Technology, U.S. Department of Commerce. 2009. "Recommended Security Controls for Federal Information Systems and Organizations." NIST Special Publication 800-53 Revision 3. <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf>.

Nyanchama, M., and S.L. Osborn. 1994. "Access Rights Administration in Role-Based Security systems." Proceedings of IFIP WG11.3 Working Conference on Database Security.

Office for Civil Rights, U.S. Department of Health and Human Services. 2003. Summary of the HIPAA Privacy Rule. *Office for Civil Rights Privacy Brief.* <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf>.

Osborn, S.L. November 1997. "Mandatory Access Control and Role-Based Access Control Revisited." Proceedings of Second ACM Workshop on Role-Based Access Control.

PCI Security Standards Council. 2009. "Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures." Version 1.2.1.

Perry, J., and P. De Fontnouvelle. 2005. "Measuring Reputational Risk: The Market Reaction to Operational Loss Announcements." *SSRN eLibrary* (October 30). <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=861364>.

PriceWaterhouseCoopers. 2008. *Société Générale: Summary of PwC Diagnosis and Analysis of the Action Plan*. 23 May 2008. <http://www.societegenerale.com/sg/file/fichierig/documentIG_5197/pricewatercooper.pdf>. Accessed February 23, 2009.

Reilly, S. 2010. "Despite WikiLeaks, Joint Chiefs Vice Chairman Endorses Information Sharing." *Federal Times*, Dec. 8, 2010. <http://www.federaltimes.com/article/20101208/DEPARTMENTS01/12080301/1001>

Rolls, D. 2008. "Establishing an Operational Context for Shared Role-Based Access Control Systems." <http://www.openroleexchange.org/files/Open_Role_Exchange_White_Paper.pdf>.

Saltzer, J. H., and M. D. Schroeder. 1975. "The Protection of Information in Computer Systems." In *Proceedings of the IEEE* 63(9):1278-1308.

Sandhu, R., E.J. Coyne, H.L. Feinstein, and C.E. Youman. 1996. "Role-Based Access Control Models." *IEEE Computer* 29(2):38-47.

Sandhu, R., D. Ferraiolo, and R. Kuhn. 2000. "The NIST Model for Role-Based Access Control: Towards a Unified Standard." In *Proceedings of the Fifth ACM Workshop on Role-Based Access Control*, 47-63.

Scott, J.T. 1999. "The Service Sector's Acquisition and Development of Information Technology: Infrastructure and Productivity." *Journal of Technology Transfer* 24:37-54.

Securities and Exchange Commission. 2008. Final Rule: Management's Report on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports; Rel. No. 33-8238. <http://www.sec.gov/rules/final/33-8238.htm>.

Sinclair, S, and S.W. Smith. 2008. Preventative Directions for Insider Threat Mitigation Via Access Control. In *Insider Attack and Cyber Security*, 165-194. <http://dx.doi.org/10.1007/978-0-387-77322-3_10>.

Stiglitz, J.E. 1988. *Economics of the Public Sector*. New York: W.W. Norton & Company.

Tassey, G. 1997. *The Economics of R&D Policy*. Westport, CT: Quorum Books.

Tassey, G. 2007. *The Technology Imperative*. Northampton, MA: Edward Elgar Publishing, Inc.

TJX Companies, Inc. January 26, 2008 Form 10-K. Filed March 26, 2008.

U.S. Census Bureau. "2007 Annual Capital Expenditures Survey: Table 2a. Capital Expenditures and Percent Change for Companies with Employees by Major Industry Sector: 2007, 2006 Revised, and 2005." <http://www.census.gov/csd/ace/xls/2007/Full Report.htm>. Released January 22, 2009.

U.S. Census Bureau. "2007 Information and Communication Technology Survey Data Release: Table 3c. Capitalized Expenditures for ICT Equipment and Computer Software for Companies with Employees by Major Industry Sector: 2007, 2006 Revised, and 2005." <http://www.census.gov/csd/ict/xls/2007/Full Report.htm>. Released February 26, 2009.

U.S. Census Bureau; generated by RTI International; using American FactFinder; "Sector 54: Professional, Scientific, and Technical Services: Industry Series: Product Lines by Kind of Business for the United States: 2002." and "Sector 51: Information: Industry Series: Product Lines by Kind of Business for the United States: 2002." <http://factfinder.census.gov>. Accessed March 22, 2009.

U.S. Code 44. 2006. *Information Security.* § 3532(b)(1). <http://www.gpoaccess.gov/uscode/index.html>. Accessed February 5, 2009.

Wilshire 5000 Index. 2010. As obtained on 8/31/2010 at http://www.wilshire.com/Indexes/Broad/Wilshire5000/Characteristics.html.

Appendix A: Survey for Identity and Access Control Managers

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 broader the 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 and the Office of Management and Budget Information and Regulatory Affairs, Office of Management and Budget, Washington, DC 20503.

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
<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): _____

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
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): _____

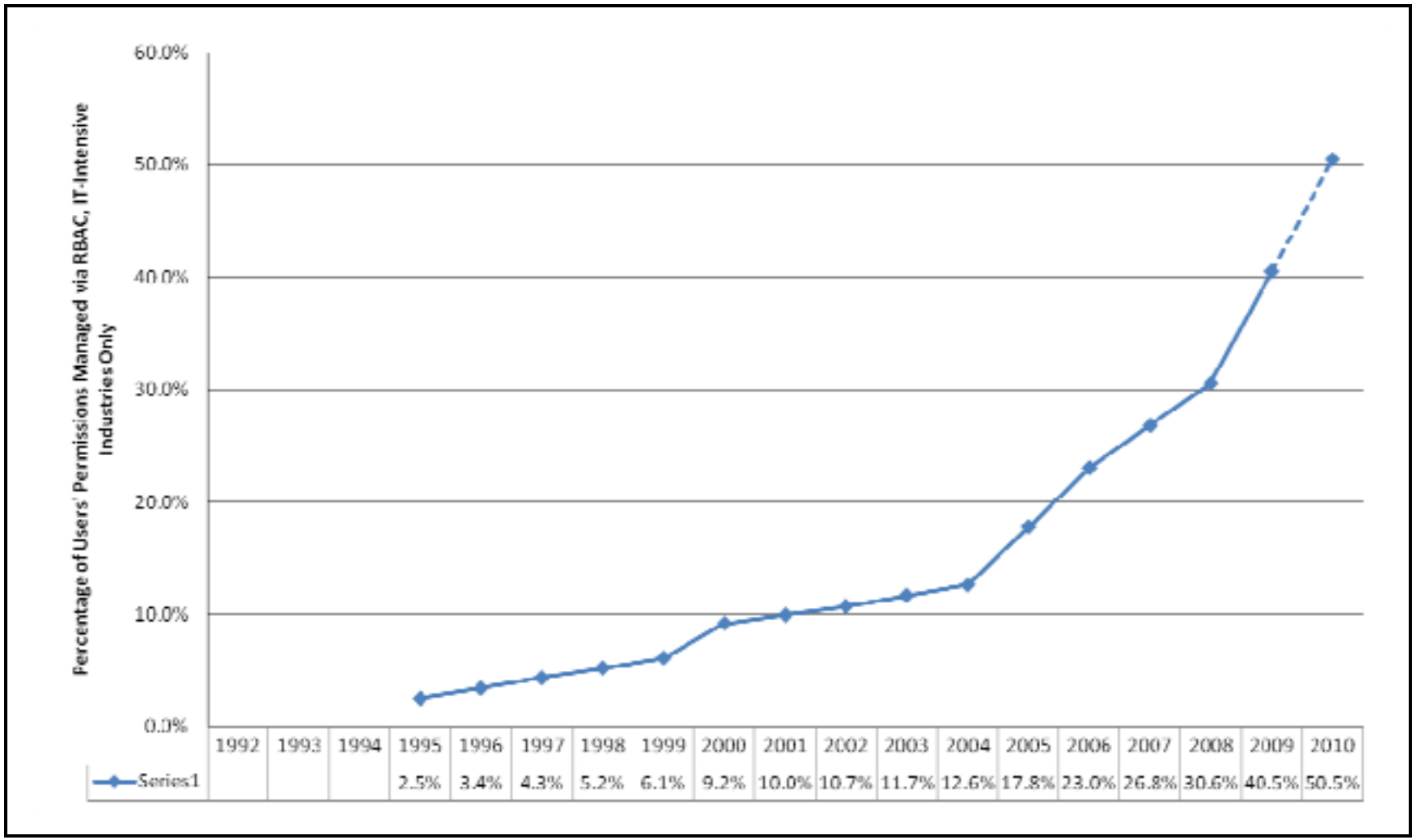
Telephone number (optional) _____

Email (optional): _____

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

Appendix B: Supplemental Analysis Tables

Figure B-1.Estimated RBAC Penetration Rate



Note: Industries were defined by 2-digit NAICS code and included utilities; manufacturing; wholesale trade; retail trade; information; finance and insurance; professional, scientific, and technical services; educational services; health care and social assistance; arts, entertainment, and recreation; other services; and public administration.

Table B-1. Times Series of Employment at Organizations with 500 or More Employees, by Industry

NAICS	Sector	Included Industry[a]	1994[b]	1995[b]	1996[b]	1997[b]	1998	1999	2000	2001
21	Mining		278,652	278,652	278,652	278,652	278,652	260,594	255,654	271,026
22	Utilities	✓	578,717	578,717	578,717	578,717	578,717	564,707	550,494	548,514
23	Construction		679,003	679,003	679,003	679,003	679,003	774,783	897,732	964,696
31–33	Manufacturing	✓	9,931,342	9,931,342	9,931,342	9,931,342	9,931,342	9,818,591	9,672,109	9,312,458
42	Wholesale trade	✓	2,035,377	2,035,377	2,035,377	2,035,377	2,035,377	2,137,745	2,225,508	2,277,095
44–45	Retail trade	✓	7,851,673	7,851,673	7,851,673	7,851,673	7,851,673	8,094,491	8,349,169	8,427,885
48–49	Transportation & warehousing		1,955,724	1,955,724	1,955,724	1,955,724	1,955,724	2,102,888	2,233,906	2,192,925
51	Information	✓	2,238,831	2,238,831	2,238,831	2,238,831	2,238,831	2,321,039	2,549,220	2,759,701
52	Finance & insurance	✓	3,889,704	3,889,704	3,889,704	3,889,704	3,889,704	4,048,969	4,049,152	4,307,387
53	Real estate & rental & leasing		504,670	504,670	504,670	504,670	504,670	550,131	584,186	632,766
54	Professional, scientific, & technical services	✓	2,040,933	2,040,933	2,040,933	2,040,933	2,040,933	2,242,784	2,407,973	2,567,560
55	Management of companies & enterprises		2,399,500	2,399,500	2,399,500	2,399,500	2,399,500	2,474,610	2,565,880	2,553,750
56	Administrative & support & waste management & remediation services		4,426,750	4,426,750	4,426,750	4,426,750	4,426,750	4,989,739	5,660,629	5,536,302
61	Educational services	✓	1,231,030	1,231,030	1,231,030	1,231,030	1,231,030	1,288,503	1,339,116	1,375,349
62	Health care & social assistance	✓	7,304,840	7,304,840	7,304,840	7,304,840	7,304,840	7,354,644	7,401,086	7,628,901
71	Arts, entertainment, & recreation	✓	475,632	475,632	475,632	475,632	475,632	506,624	558,392	587,284
72	Accommodation & foodservices		3,658,508	3,658,508	3,658,508	3,658,508	3,658,508	3,789,408	3,926,848	3,973,106
81	Other services (except public administration)	✓	688,460	688,460	688,460	688,460	688,460	723,058	748,720	776,852
92	Public administration (federal gov't)	✓	2,643,940	2,580,430	2,536,464	2,492,497	2,447,496	2,449,089	2,425,898	2,411,630
	Total		54,836,688	54,773,178	54,729,212	54,685,245	54,616,842	56,492,397	58,401,672	59,105,187
	Subtotal for included industries		40910479	40846969	40803002.5	40759036	40,714,035	41,550,244	42,276,837	42,980,616

(continued)

Table B-1. Times Series of Employment at Organizations with 500 or More Employees, by Industry (continued)

NAICS	Sector	Included Industry[a]	2002	2003	2004	2005	2006	2007	2008[c]	2009[c]
21	Mining		261,480	253,576	259,156	277,537	309,795	418,609	418,609	418,609
22	Utilities	✓	537,664	532,443	527,221	523,931	505,268	512,412	512,412	512,412
23	Construction		946,025	894,227	902,043	939,576	1,074,142	1,077,482	1,077,482	1,077,482
31–33	Manufacturing	✓	8,298,668	8,030,010	7,741,481	7,628,545	7,575,462	7,402,462	7,402,462	7,402,462
42	Wholesale trade	✓	2,180,763	2,223,480	2,269,755	2,331,700	2,344,969	2,329,016	2,329,016	2,329,016
44–45	Retail trade	✓	8,458,586	8,463,187	8,879,752	9,030,694	9,453,604	9,621,300	9,621,300	9,621,300
48–49	Transportation & warehousing		2,089,679	2,515,586	2,527,922	2,581,515	2,676,777	2,777,353	2,777,353	2,777,353
51	Information	✓	2,632,117	2,678,380	2,563,528	2,512,310	2,502,240	2,522,129	2,522,129	2,522,129
52	Finance & insurance	✓	4,451,290	4,399,089	4,373,555	4,302,969	4,463,233	4,414,232	4,414,232	4,414,232
53	Real estate & rental & leasing		630,317	628,651	643,991	681,017	695,767	720,696	720,696	720,696
54	Professional, scientific, & technical services	✓	2,523,201	2,793,556	2,909,470	2,948,040	3,096,079	3,184,574	3,184,574	3,184,574
55	Management of companies & enterprises		2,536,367	2,530,947	2,482,233	2,518,437	2,563,968	2,737,814	2,737,814	2,737,814
56	Administrative & support & waste management & remediation services		5,013,669	5,045,753	5,125,110	5,660,565	6,271,088	6,259,488	6,259,488	6,259,488
61	Educational services	✓	1,426,573	1,471,203	1,563,695	1,584,946	1,645,568	1,675,703	1,675,703	1,675,703
62	Health care & social assistance	✓	7,755,218	8,012,865	8,149,160	8,276,386	8,504,967	8,807,758	8,807,758	8,807,758
71	Arts, entertainment, & recreation	✓	607,866	596,281	609,820	655,818	675,571	695,324	695,324	695,324
72	Accommodation & foodservices		3,962,289	4,090,179	4,182,144	4,414,317	4,532,320	4,710,142	4,710,142	4,710,142
81	Other services (except public administration)	✓	750,209	731,041	743,650	777,986	794,978	842,853	842,853	842,853
92	Public administration (federal gov't)	✓	2,426,467	2,453,158	2,445,287	2,437,558	2,438,657	2,462,127	2,518,101	2,518,101
	Total		57,488,448	58,343,612	58,898,973	60,083,847	62,124,453	63,171,474	63,227,448	63,227,448
	Subtotal for Included Industries		42,048,622	42,384,693	42,776,374	43,010,883	44,000,596	44,469,890	44,525,864	44,525,864

[a] Industry inclusion was determined by multiple survey responses within a given industry (see Chapter 5).

[b] This data series was not collected 1994–1997 and the values for 1998 were assumed to be representative of previous years, with the exception of NAICS 92.

[c] Data for 2008 and 2009 are not yet available and the values for 2007 were assumed to be representative of those for 2008 and 2009, with the exception of NAICS 92 which has 2008 data available.

Sources: U.S. Census Bureau, Government Employment and Payroll. 2010. "Federal Government Civilian Employment: Total Full-Time Employees. 1998–2007."Accessed September 29, 2010. http://www.census.gov/govs/apes/.

U.S. Census Bureau, Statistics of U.S. Businesses. 2010. "Number of Firms, Number of Establishments, Employment and Annual Payroll by Employment Size of the Enterprise for the United States, All Industries: 1998–2007." Accessed October 16th, 2009 and September 17th, 2010. http://www.census.gov/econ/susb/.

Table B-2. GDP Implicit Price Deflator

Year	GDP in Billions of Current Dollars	GDP in Billions of Chained 2005 Dollars	GDP Deflator	2009 Deflator
1990	5,800.5	8,033.9	0.7220	0.6587
1991	5,992.1	8,015.1	0.7476	0.6820
1992	6,342.3	8,287.1	0.7653	0.6982
1993	6,667.4	8,523.4	0.7822	0.7136
1994	7,085.2	8,870.7	0.7987	0.7287
1995	7,414.7	9,093.7	0.8154	0.7438
1996	7,838.5	9,433.9	0.8309	0.7580
1997	8,332.4	9,854.3	0.8456	0.7714
1998	8,793.5	10,283.5	0.8551	0.7801
1999	9,353.5	10,779.8	0.8677	0.7916
2000	9,951.5	11,226.0	0.8865	0.8087
2001	10,286.2	11,347.2	0.9065	0.8270
2002	10,642.3	11,553.0	0.9212	0.8404
2003	11,142.1	11,840.7	0.9410	0.8585
2004	11,867.8	12,263.8	0.9677	0.8828
2005	12,638.4	12,638.4	1.0000	0.9123
2006	13,398.9	12,976.2	1.0326	0.9420
2007	14,061.8	13,228.9	1.0630	0.9697
2008	14,369.1	13,228.8	1.0862	0.9909
2009	14,119.0	12,880.6	1.0961	1.0000

Source: GDP implicit price deflator (BEA, 2009)

Table B-3. Time Series of Mean Hourly Wage Rates, by Industry

NAICS	Sector	1994[a]	1995[a]	1996[a]	1997[a]	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
22	Utilities	16.62	16.62	16.62	16.62	16.62	17.61	18.36	19.03	25.57	25.90	25.83	25.83	26.80	27.83	29.10	29.58
23	Construction	15.76	15.76	15.76	15.76	15.76	17.33	17.66	18.14	18.92	19.23	19.44	19.69	20.17	20.83	21.68	22.36
31–33	Manufacturing	15.15	15.15	15.15	15.15	15.15	16.04	16.74	17.45	17.76	18.35	18.57	18.87	19.38	20.09	20.80	21.43
42	Wholesale trade	15.94	15.94	15.94	15.94	15.94	16.99	17.76	18.38	19.71	20.24	20.40	20.87	21.60	22.55	23.41	24.00
44–45	Retail trade	9.13	9.13	9.13	9.13	9.13	9.81	10.02	10.41	12.15	12.42	12.53	12.67	13.00	13.37	13.73	13.79
48–49	Transportation and warehousing	16.62	16.62	16.62	16.62	16.62	17.61	18.36	19.03	17.64	18.44	18.61	19.02	19.39	20.01	20.35	20.56
51	Information	14.65	14.65	14.65	14.65	14.65	15.54	16.32	16.89	22.59	23.12	23.62	24.06	24.93	26.25	27.56	28.40
52	Finance and insurance	16.89	16.89	16.89	16.89	16.89	18.75	19.39	19.83	22.12	22.49	23.04	23.65	24.59	25.57	26.65	27.31
53	Real estate and rental and leasing	16.89	16.89	16.89	16.89	16.89	18.75	19.39	19.83	15.25	15.69	15.99	16.76	17.32	17.99	18.61	19.16
54	Professional, scientific, and technical services	14.65	14.65	14.65	14.65	14.65	15.54	16.32	16.89	26.36	27.11	27.63	28.15	29.13	30.47	31.75	32.81
55	Management of companies and enterprises	16.89	16.89	16.89	16.89	16.89	18.75	19.39	19.83	25.11	25.72	26.40	27.13	28.41	29.93	31.31	32.39
56	Administrative and support and waste management and remediation services	14.65	14.65	14.65	14.65	14.65	15.54	16.32	16.89	12.67	13.42	13.56	14.19	14.56	15.11	15.69	16.17
61	Educational services	14.65	14.65	14.65	14.65	14.65	15.54	16.32	16.89	18.78	19.30	19.56	20.12	20.94	21.62	22.56	23.09
62	Health care and social assistance	14.65	14.65	14.65	14.65	14.65	15.54	16.32	16.89	17.54	18.13	18.42	18.94	19.74	20.48	21.31	21.84
71	Arts, entertainment, and recreation	14.65	14.65	14.65	14.65	14.65	15.54	16.32	16.89	12.62	13.03	13.14	13.43	14.07	14.58	15.08	15.41
72	Accommodation and food service	9.13	9.13	9.13	9.13	9.13	9.81	10.02	10.41	8.87	8.98	9.06	9.18	9.45	9.87	10.26	10.56
81	Other services (except public administration)	14.65	14.65	14.65	14.65	14.65	15.54	16.32	16.89	13.70	14.00	14.30	14.76	15.23	15.78	16.34	16.76
92	Public administration	16.75	16.75	16.75	16.75	16.75	17.66	18.48	19.10	19.62	20.31	20.71	21.28	22.13	23.00	23.81	24.62
	Network and systems administrator wage, cross-industry average	24.08	24.08	24.08	24.08	24.08	24.08	25.81	27.14	27.70	28.43	29.55	30.39	31.37	32.62	33.45	34.10
	Management occupations, computer systems, cross-industry average	35.79	35.79	35.79	35.79	35.79	35.79	38.58	40.33	43.48	46.13	48.13	49.21	51.56	54.75	57.07	58.00
	Management occupations, cross-industry average	31.13	31.13	31.13	31.13	31.13	31.13	32.78	34.04	37.92	39.80	41.12	42.52	44.20	46.22	48.23	49.47

[a] Data for 1994 through 1997 were assumed to be the same as those for 1998.

Source: Bureau of Labor Statistics, Department of Labor, 2010. "Occupational Employment Statistics (OES) Survey: National Cross-Industry Estimates 1998–1999. Accessed September 20, 2010. http:/stat.bls.gov/oes/home.htm.

Table B-4. Time Series of Deflated Fully-Loaded Mean Hourly Wage Rate, by Industry

NAICS	Sector	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
22	Utilities	42.60	42.60	42.60	42.60	42.60	44.49	45.41	46.01	60.85	60.34	58.52	56.63	56.90	57.40	58.73	59.16
23	Construction	40.41	40.41	40.41	40.41	40.41	43.79	43.67	43.87	45.03	44.80	44.04	43.17	42.82	42.96	43.76	44.72
31–33	Manufacturing	38.83	38.83	38.83	38.83	38.83	40.54	41.41	42.20	42.27	42.75	42.07	41.37	41.15	41.43	41.98	42.86
42	Wholesale trade	40.87	40.87	40.87	40.87	40.87	42.93	43.93	44.45	46.90	47.15	46.21	45.75	45.86	46.51	47.25	48.00
44–45	Retail trade	23.41	23.41	23.41	23.41	23.41	24.78	24.77	25.17	28.93	28.94	28.39	27.78	27.60	27.57	27.71	27.58
48–49	Transportation and warehousing	42.60	42.60	42.60	42.60	42.60	44.49	45.41	46.01	41.99	42.96	42.16	41.70	41.17	41.27	41.07	41.12
51	Information	37.56	37.56	37.56	37.56	37.56	39.25	40.36	40.85	53.77	53.86	53.51	52.75	52.93	54.14	55.62	56.80
52	Finance and insurance	43.30	43.30	43.30	43.30	43.30	47.38	47.96	47.97	52.65	52.40	52.20	51.85	52.21	52.74	53.79	54.62
53	Real estate and rental and leasing	43.30	43.30	43.30	43.30	43.30	47.38	47.96	47.97	36.28	36.55	36.22	36.74	36.77	37.10	37.56	38.32
54	Professional, scientific, and technical services	37.56	37.56	37.56	37.56	37.56	39.25	40.36	40.85	62.73	63.16	62.59	61.71	61.85	62.84	64.08	65.62
55	Management of companies and enterprises	43.30	43.30	43.30	43.30	43.30	47.38	47.96	47.97	59.76	59.92	59.81	59.48	60.32	61.73	63.19	64.78
56	Administrative and support and waste management and remediation services	37.56	37.56	37.56	37.56	37.56	39.25	40.36	40.85	30.16	31.27	30.72	31.11	30.91	31.16	31.67	32.34
61	Educational services	37.56	37.56	37.56	37.56	37.56	39.25	40.36	40.85	44.69	44.96	44.31	44.11	44.46	44.59	45.53	46.18
62	Health care and social assistance	37.56	37.56	37.56	37.56	37.56	39.25	40.36	40.85	41.73	42.24	41.73	41.52	41.91	42.24	43.01	43.68
71	Arts, entertainment, and recreation	37.56	37.56	37.56	37.56	37.56	39.25	40.36	40.85	30.03	30.36	29.77	29.44	29.87	30.07	30.44	30.82
72	Accommodation and food service	23.41	23.41	23.41	23.41	23.41	24.78	24.77	25.17	21.10	20.92	20.52	20.13	20.06	20.36	20.71	21.12
81	Other services (except public administration)	37.56	37.56	37.56	37.56	37.56	39.25	40.36	40.85	32.60	32.62	32.40	32.36	32.34	32.55	32.98	33.52
92	Public administration	42.94	42.94	42.94	42.94	42.94	44.62	45.70	46.19	46.70	47.32	46.92	46.65	46.98	47.44	48.06	49.24
	Network and systems administrator wage, cross-industry average	60.84	60.84	60.84	60.84	60.84	60.84	63.83	65.64	65.92	66.23	66.94	66.62	66.60	67.28	67.51	68.20
	Management occupations, computer systems, cross-industry average	90.43	90.43	90.43	90.43	90.43	90.43	95.41	97.53	103.48	107.47	109.04	107.88	109.47	112.92	115.19	116.00
	Management occupations, cross-industry average	78.65	78.65	78.65	78.65	78.65	78.65	81.07	82.32	90.25	92.72	93.15	93.22	93.84	95.33	97.34	98.94

Notes: All dollar values have been adjusted to real 2009 dollars using the gross domestic product (GDP) implicit price deflator (BEA, 2009). Fully loaded wage rates are two times the average wage rate to incorporate other costs of employment. Wages between 1998 and 2001 are based on SIC code divisions to provide the appropriate NAICS sector estimate.

Source: Bureau of Labor Statistics, Department of Labor, 2010. "Occupational Employment Statistics (OES) Survey: National Cross-Industry Estimates 1998–1999. Accessed September 20, 2010. http:/stat.bls.gov/oes/home.htm.

Table B-5. Estimated RBAC Adoption (Employees with at Least Some Permissions Managed via Roles)

NAICS	Sector	1995	1996	1997	1998	1999	2000	2001	2002
22	Utilities	14,665	19,842	25,019	30,196	34,516	50,668	54,611	57,575
23	Construction	—	—	—	—	—	—	—	—
31–33	Manufacturing	251,668	340,507	429,346	518,185	600,133	890,237	927,172	888,649
42	Wholesale trade	51,578	69,785	87,992	106,199	130,663	204,839	226,713	233,523
44–45	Retail trade	198,968	269,204	339,439	409,675	494,752	768,471	839,101	905,774
48–49	Transportation and warehousing	—	—	—	—	—	—	—	—
51	Information	56,734	76,761	96,788	116,815	141,867	234,634	274,763	281,856
52	Finance and insurance	98,568	133,363	168,158	202,952	247,481	372,691	428,854	476,659
53	Real estate and rental and leasing	—	—	—	—	—	—	—	—
54	Professional, scientific, and technical services	51,719	69,976	88,233	106,489	137,084	221,634	255,633	270,193
55	Management of companies and enterprises	—	—	—	—	—	—	—	—
56	Administrative and support and waste management and remediation services	—	—	—	—	—	—	—	—
61	Educational services	31,195	42,207	53,219	64,231	78,756	123,254	136,933	152,762
62	Health care and social assistance	185,111	250,455	315,799	381,143	449,531	681,208	759,552	830,455
71	Arts, entertainment, and recreation	12,053	16,308	20,562	24,817	30,966	51,395	58,471	65,092
72	Accommodation and food service	—	—	—	—	—	—	—	—
81	Other services (except public administration)	17,446	23,605	29,763	35,922	44,195	68,913	77,345	80,335
92	Public administration	65,390	86,966	107,754	127,702	149,693	223,284	240,108	259,834
	Total	1,035,096	1,398,978	1,762,073	2,124,327	2,539,638	3,891,231	4,279,258	4,502,707

(continued)

Table B-5. Estimated RBAC Adoption (Employees with at Least Some Permissions Managed via Roles) (continued)

NAICS	Sector	2003	2004	2005	2006	2007	2008	2009
22	Utilities	62,044	66,415	93,307	116,317	137,266	156,570	207,562
23	Construction	—	—	—	—	—	—	—
31–33	Manufacturing	935,719	975,212	1,358,570	1,743,934	1,982,986	2,261,863	2,998,511
42	Wholesale trade	259,097	285,926	415,253	539,831	623,901	711,644	943,413
44–45	Retail trade	986,196	1,118,602	1,608,279	2,176,298	2,577,373	2,939,842	3,897,295
48–49	Transportation and warehousing	—	—	—	—	—	—	—
51	Information	312,106	322,933	447,418	576,036	675,633	770,651	1,021,637
52	Finance and insurance	512,616	550,946	766,317	1,027,473	1,182,493	1,348,793	1,788,071
53	Real estate and rental and leasing	—	—	—	—	—	—	—
54	Professional, scientific, and technical services	325,527	366,512	525,017	712,743	853,090	973,064	1,289,974
55	Management of companies and enterprises	—	—	—	—	—	—	—
56	Administrative and support and waste management and remediation services	—	—	—	—	—	—	—
61	Educational services	171,436	196,982	282,263	378,823	448,891	512,020	678,776
62	Health care and social assistance	933,721	1,026,568	1,473,944	1,957,914	2,359,439	2,691,259	3,567,754
71	Arts, entertainment, and recreation	69,483	76,820	116,795	155,522	186,265	212,460	281,655
72	Accommodation and food service	—	—	—	—	—	—	—
81	Other services (except public administration)	85,187	93,679	138,552	183,011	225,785	257,538	341,414
92	Public administration	285,861	308,038	434,105	561,399	659,559	769,420	1,020,006
	Total	4,938,994	5,388,635	7,659,820	10,129,304	11,912,681	13,605,125	18,036,067

Table B-6. Economic Benefits from Reduced Employee Downtime from More Efficient Provisioning (millions, 2009$)

NAICS	Sector	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
22	Utilities	0.17	0.40	0.52	0.64	0.79	1.06	1.32	1.86	1.97	2.05	2.47	3.26	3.98	4.71	5.88
23	Construction	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
31–33	Manufacturing	2.67	7.22	9.11	10.99	12.38	16.86	20.95	20.96	21.30	21.96	26.37	34.87	42.18	48.67	61.58
42	Wholesale trade	0.58	1.56	1.96	2.37	2.78	4.03	5.24	5.90	6.34	6.88	8.76	11.96	14.78	17.23	21.70
44–45	Retail trade	1.27	3.44	4.34	5.24	6.12	8.55	11.05	13.78	14.95	16.32	20.69	28.53	35.80	41.76	51.50
48–49	Transportation and warehousing	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
51	Information	0.58	1.57	1.99	2.40	2.77	4.15	5.68	8.17	8.74	9.28	11.10	14.80	18.51	21.97	27.80
52	Finance and insurance	1.17	3.15	3.98	4.80	5.83	8.12	10.50	13.02	14.16	15.16	18.65	25.58	31.83	37.19	46.79
53	Real estate and rental and leasing	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
54	Professional, scientific, and technical services	0.53	1.44	1.81	2.18	2.61	3.95	5.33	9.01	10.28	11.83	15.03	20.91	26.88	31.96	40.56
55	Management of companies and enterprises	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
56	administrative and support and waste management and remediation services	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
61	Educational services	0.32	0.87	1.09	1.32	1.53	2.23	2.90	3.54	3.98	4.46	5.77	8.03	10.08	11.95	15.02
62	Health care and social assistance	1.90	5.14	6.48	7.82	8.91	12.46	16.08	18.12	20.35	22.34	28.36	39.28	49.81	59.33	74.67
71	Arts, entertainment, and recreation	0.12	0.33	0.42	0.51	0.60	0.91	1.23	1.01	1.12	1.19	1.56	2.22	2.81	3.31	4.16
72	Accommodation and food service	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
81	Other services (except public administration)	0.18	0.48	0.61	0.74	0.86	1.25	1.63	1.40	1.47	1.58	2.05	2.84	3.63	4.35	5.48
92	Public administration	0.77	2.04	2.53	3.00	3.38	4.66	5.85	6.38	7.05	7.61	9.46	12.77	15.82	18.76	24.06
	Total	10.25	27.65	34.84	42.00	48.55	68.22	87.75	103.16	111.72	120.66	150.26	205.04	256.09	301.20	379.21

Notes: All dollar values have been adjusted to real 2009 dollars using the gross domestic product (GDP) implicit price deflator (BEA, 2009).

Table B-7. Economic Benefits of More Efficient Provisioning by Network and Systems Administrators (millions, 2009$)

Year	Employees Managed under RBAC	IT Labor Cost per Hour (2009$)	Labor Hours Saved per Employee	Economic Benefits (millions, 2009$)
1995	1,035,096	60.8	0.035	1.10
1996	1,398,978	60.8	0.035	2.59
1997	1,762,073	60.8	0.035	3.36
1998	2,124,327	60.8	0.035	4.13
1999	2,539,638	60.8	0.035	4.96
2000	3,891,231	63.8	0.035	7.18
2001	4,279,258	65.6	0.035	9.37
2002	4,502,707	65.9	0.035	10.12
2003	4,938,994	66.2	0.035	10.93
2004	5,388,635	66.9	0.035	12.09
2005	7,659,820	66.6	0.035	15.20
2006	10,129,304	66.6	0.035	20.71
2007	11,912,681	67.3	0.035	25.92
2008	13,605,125	67.5	0.035	30.11
2009	18,036,067	68.2	0.035	37.72

Table B-8. Economic Benefits of More Efficient Access Control Policy Maintenance (millions, 2009$)

Year	Employees Managed under RBAC (Year End)	IT Labor Cost per Hour (2009$)	Business Managers Labor Cost per Hour (2009$)	Value per Employee (2009$)	Employees (Adjusted for Annual Adoption Rate)	Economic Benefits (millions, 2009$)
1992	—	—	—	—	—	—
1993	—	—	—	—	—	—
1994	—	75.63	78.65	89.77	—	—
1995	1,035,096	75.63	78.65	89.77	517,548	46.46
1996	1,398,978	75.63	78.65	89.77	1,217,037	109.26
1997	1,762,073	75.63	78.65	89.77	1,580,525	141.89
1998	2,124,327	75.63	78.65	89.77	1,943,200	174.44
1999	2,539,638	75.63	78.65	89.77	2,331,982	209.35
2000	3,891,231	79.62	81.07	93.72	3,215,434	301.35
2001	4,279,258	81.59	82.32	95.70	4,085,244	390.94
2002	4,502,707	84.70	90.25	101.51	4,390,982	445.74
2003	4,938,994	86.85	92.72	104.18	4,720,850	491.80
2004	5,388,635	87.99	93.15	105.19	5,163,814	543.16
2005	7,659,820	87.25	93.22	104.69	6,524,227	683.00
2006	10,129,304	88.04	93.84	105.53	8,894,562	938.65
2007	11,912,681	90.10	95.33	107.68	11,020,992	1,186.73
2008	13,605,125	91.35	97.34	109.49	12,758,903	1,396.95
2009	18,036,067	92.10	98.94	110.75	15,820,596	1,752.11

Table B-9. RBAC Adoption Costs (millions, 2009$)

Year	Employees Managed under RBAC	IT Labor Cost per Hour (2009$)	Business Managers Labor Cost per Hour (2009$)	IT Labor, Hours per Employee	Business Operations Labor, Hours per Employee	Labor Costs (million, 2009$)	Non-Labor Costs (million, 2009$)
1994	—	75.63	78.65	0.75	1.33	111.87	40.74
1995	1,035,096	75.63	78.65	0.75	1.33	95.27	15.85
1996	1,398,978	75.63	78.65	0.75	1.33	58.91	16.35
1997	1,762,073	75.63	78.65	0.75	1.33	58.77	16.85
1998	2,124,327	75.63	78.65	0.75	1.33	64.46	19.47
1999	2,539,638	75.63	78.65	0.75	1.33	168.53	56.94
2000	3,891,231	79.62	81.07	0.75	1.33	119.40	21.00
2001	4,279,258	81.59	82.32	0.75	1.33	47.73	15.10
2002	4,502,707	84.70	90.25	0.75	1.33	67.39	23.80
2003	4,938,994	86.85	92.72	0.75	1.33	84.31	24.97
2004	5,388,635	87.99	93.15	0.75	1.33	317.52	97.33
2005	7,659,820	87.25	93.22	0.75	1.33	457.47	108.48
2006	10,129,304	88.04	93.84	0.75	1.33	385.86	85.11
2007	11,912,681	90.10	95.33	0.75	1.33	336.47	84.16
2008	13,605,125	91.35	97.34	0.75	1.33	699.92	194.44
2009	18,036,067	92.10	98.94	0.75	1.33	893.49	200.96

Note: See also Chapter 5.

Table B-10. Time Series of Net Economic Benefits

Year	R&D Expenditures (millions, 2000$)	R&D Expenditures (millions, 2009$)	End Users' Customization and Implementation Costs (millions, 2009$)	End Users Operation Benefits (millions, 2009$)	Benefits, net of Installation (millions, 2009$)	Net Benefits (millions, 2009$)
1992	—	—	—	—	—	—
1993	—	—	—	—	—	—
1994	—	—	−152.6	0.0	−152.6	−152.6
1995	—	—	−111.1	57.8	−53.3	−53.3
1996	−5.05	−6.24	−75.3	139.5	64.2	58.0
1997	−5.05	−6.24	−75.6	180.1	104.5	98.2
1998	−5.05	−6.24	−83.9	220.6	136.6	130.4
1999	−5.05	−6.24	−225.5	262.9	37.4	31.2
2000	−5.05	−6.24	−140.4	376.7	236.3	230.1
2001	−5.05	−6.24	−62.8	488.1	425.2	419.0
2002	−5.05	−6.24	−91.2	559.0	467.8	461.6
2003	−5.05	−6.24	−109.3	623.1	513.8	507.6
2004	−5.05	−6.24	−414.8	685.4	270.6	264.3
2005	−5.05	−6.24	−565.9	860.3	294.3	288.1
2006	−5.05	−6.24	−471.0	1,180.4	709.4	703.2
2007	—	—	−420.6	1,488.7	1,068.1	1,068.1
2008	—	—	−894.4	1,751.6	857.2	857.2
2009	—	—	−1,094.4	2,198.2	1,103.7	1,103.7
Total	**−55.6**	**−68.7**	**−4,988.9**	**11,072.3**	**6,083.4**	**6,014.7**

Table B-11. Time Series of Net Economic Benefits Attributable to NIST

Year	R&D Expenditures (millions, 2000$)	R&D Expenditures (millions, 2009$)	End Users' Customization and Implementation Costs (millions, 2009$)	End Users Operation Benefits (millions, 2009$)	Benefits, net of Installation (millions, 2009$)	Net Benefits (millions, 2009$)	Total Change in Net Benefits (millions, 2009$)	NIST Expenditures (2000$)	NIST Expenditures (millions, 2009$)	Benefits Attributable to NIST (millions, 2009$)
1992	—	—	—	—	—	—	0.0	0.1	0.1	−0.1
1993	—	—	—	—	—	—	0.0	0.1	0.1	−0.1
1994	—	—	—	—	—	—	−152.6	0.2	0.2	−152.9
1995	—	—	−152.6	0.0	−152.6	−152.6	99.3	0.5	0.6	98.7
1996	—	—	−111.1	57.8	−53.3	−53.3	111.3	0.5	0.6	110.7
1997	−5.50	−6.80	−75.3	139.5	64.2	57.4	40.8	0.4	0.5	40.3
1998	−5.50	−6.80	−75.6	180.1	104.5	97.7	32.7	0.3	0.4	32.3
1999	−5.50	−6.80	−83.9	220.6	136.6	129.8	−98.7	0.0	0.0	−98.7
2000	−5.50	−6.80	−225.5	262.9	37.4	30.6	199.5	0.0	0.0	199.4
2001	−5.50	−6.80	−140.4	376.7	236.3	229.5	189.5	0.0	0.0	189.4
2002	−5.50	−6.80	−62.8	488.1	425.2	418.4	43.2	—	—	43.2
2003	−5.50	−6.80	−91.2	559.0	467.8	461.0	46.5	—	—	46.5
2004	−5.50	−6.80	−109.3	623.1	513.8	507.0	−242.7	—	—	−242.7
2005	−5.50	−6.80	−414.8	685.4	270.6	263.8	24.3	—	—	24.3
2006	−5.50	−6.80	−565.9	860.3	294.3	287.5	415.7	—	—	415.7
2007	−5.50	−6.80	−471.0	1,180.4	709.4	702.6	365.5	—	—	365.5
2008	—	—	−420.6	1,488.7	1,068.1	1,068.1	−210.9	—	—	−210.9
2009	—	—	−894.4	1,751.6	857.2	857.2	246.5	—	—	246.5
Total	**−60.5**	**−74.8**	**−3,894.5**	**8,874.1**	**4,979.6**	**4,904.8**	**1,109.8**	**2.1**	**2.6**	**1,107.3**