

**OMB Control No. 0693-0033**  
**Expiration Date: 10/31/2012**

**NIST Role-Based Access Control (RBAC) Study Survey:**  
**Economics of Access Control Policy Models for Identity Management**

**1. Explain who will be surveyed and why the group is appropriate to survey.**

RTI International<sup>1</sup> will field an Internet survey to active professionals engaged in identity management (IdM), such as information technology (IT) security managers, senior IdM systems administrators, and information security architects. The survey is intended for managers that are tasked with designing, implementing, and maintaining their organizations' access control policies and procedures for user authentication and authorization. These stakeholders manage information security and user authorization and authentication systems. They also manage the governance, risk, and compliance activities associated with federal privacy and separation of duties regulations. Respondents will be asked to answer a series of questions about how role-based access control (RBAC) policy models developed by NIST improved the efficiency and effectiveness of their network operations. The majority of the target population is employed by firms with more than 500 employees or in large government agencies.

Groups agreeing to support the survey include the Health Information Management Systems Society (HIMSS), the Information Systems Audit and Control Association (ISACA), and the Burton Group. It is expected that 50,000 U.S. members of these organizations in the US will be aware of the survey.

It is not possible to project actual response rates with great accuracy; however, Internet surveys of interest to professional societies routinely achieve a response rate of 3%. If a 3% response rate is achieved, the total number of responses would be 1,500. [This rate differs from the industry coverage rate, which reflects the total number of employees at responding organizations relative total employment at firms with greater than 500 employees.]

The survey instrument will enable RTI to measure:

- Access policy models in use by IdM managers;
- RBAC usage and adoption, by industry, over the period from 1999 to present;
- Economic benefits of using RBAC for managing users IT permissions, relative to if RBAC were not used and managers instead used simple access control lists (ACLs);
- Economic benefits for designing and maintaining RBAC policies, relative to if ACLs were used; and
- Economic benefits for using RBAC for governance, risk, and compliance activities.

All potential survey respondents are highly likely to be familiar with the technical terms and

---

<sup>1</sup> RTI International is the trade name of the Research Triangle Institute.

concepts included in the survey. Respondents will be screened by indicating whether they use RBAC and if they are sufficiently familiar with a line of inquiry to participate. Those that are not will exit the survey. Respondents will be asked to indicate their stakeholder group and geographic location.

**2. Explain how the survey was developed including consultation with interested parties, pretesting, and responses to suggestions for improvement.**

The survey instrument was developed internally at RTI by a team of technology economists in consultation with cybersecurity and access control policy experts at NIST and in industry. The question topics originate with a series of informal conversations the project team held with a variety of industry representatives from user communities and large vendors. The survey was also reviewed by HIMSS, ISACA, and the Burton Group. NIST's economics and Information Technology Laboratory staff also reviewed and approved the survey.

The survey was pre-tested by RTI with potential respondents, who indicated that the questions were appropriate and who provided the estimated time to complete the survey. All reviewers provided minor wording changes, which were incorporated into the final version. The instrument includes yes/no, short answer, and tabular questions to capture information on adoption and usage of RBAC.

**3. Explain how the survey will be conducted, how customers will be sampled if fewer than all customers will be surveyed, expected response rate, and actions your agency plans to take to improve the response rate.**

RTI will field an Internet survey targeted to a broad audience of IdM professionals to capture benefits of RBAC and measure RBAC adoption. The survey will be promoted via many channels Burton Group's Catalyst Conference series, emails to ISACA and HIMSS members, and social media sites for IdM maintained by major professional societies. The survey and its results will be of great interest to respondents because of the timeliness of its topic areas in the user provisioning costs and issues surrounding governance, risk, and compliance.

At this time, RTI is coding the Internet survey. Once the survey is operational, it will be uploaded to a website that will be housed on RTI's encrypted servers. Our security policy will ensure that information provided by respondents is secure. The survey URL will be <https://accesscontrolsurvey.rti.org> and should be operational in mid-June.

Total respondent burden time is estimated to be 15 minutes for non-RBAC users and up to 30 minutes for RBAC users, including reviewing the survey instrument and directions. If the respondent so chooses by indication on the web survey, RTI may conduct a follow-up telephone call to collect qualitative information that is related to the costs and benefits of RBAC that can

not be easily obtained in a survey format. If respondents have difficulty with the website, they

may choose to have a survey in MS Word format emailed to them for completion.

As discussed above, our population of interest is professionals who manage employee's access to information technology. There is no directory or list that provides a comprehensive list of this population. However, we assume that over 80% of these individuals are connected to societies that provide training, certification, conferences, and information on best management practices within this field.<sup>2</sup> Therefore, we will rely on these information channels to publicize the survey, ensuring the broadest possible segment of the population as possible. All individuals notified will be allowed to participate in the web-based survey.

The Burton Group, HIMSS, and ISACA will promote the survey. The membership of these scientific societies is comprised of individuals employed by companies and institutions in each of our stakeholder groups. They will direct their members to RTI's survey website through e-mail alerts, mentions in member publications, and links on their homepages. In addition, RTI will advertise this survey directly to materials scientists using listservs and web forums that are used by individuals in each of these stakeholder groups. The sum of these actions should significantly improve response rates by alerting as many people as possible to the survey.

#### **4. Describe how the results of the survey will be analyzed and used to generalize the results to the entire customer population.**

We will extrapolate survey data using total US employment by industry at firms with more than 500 employees. Smaller companies are unlikely to have adopted RBAC. The survey includes questions on number of users and employees at their organization. The sum of responses will be extrapolated to national estimates using employment data. Since the aim of this study is to estimate the impact of RBAC for managing IT permissions, the ideal variable to use when creating the cut-off sample would be number of employees.

---

<sup>2</sup> The 80% cut-off level is based on OMB's suggested methodology and is intended to ensure that the sample provides the minimum mean square error estimate for the total value of the variable used to specify the coverage.