2010 Access Governance Trends Survey

Sponsored by Aveksa

Independently conducted by Ponemon Institute LLC

Publication Date: April 19, 2010

2010 Access Governance Trends Survey

Study of IT Practitioners in Multinational Organizations
Ponemon Institute, April 19, 2010

I. Executive Summary

When employees, temporary employees, contractors and partners have inappropriate access to information resources – that is, access that violates security policies and regulations or that is inappropriate for their current jobs – companies are subject to serious compliance and business risks. To mitigate this risk, companies need a governance framework that helps to ensure access to corporate information resources is appropriate and avoids any misuse that could negatively impact their organization.

Aveksa and Ponemon Institute are pleased to present the results of the *2010 Access Governance Trends Survey*. This is the second study to examine access governance practices. In this study, we surveyed 728 experienced IT practitioners from U.S.-based multinational corporations and governmental organizations. The first access governance study was also sponsored by Aveksa and published in 2008.[1]

The overall objective of this second study is to track the perspectives of IT security and compliance practitioners about how well they are achieving access governance within their organizations. Among the numerous questions this study seeks to answer are:

- How do organizations determine who should have access to information resources and what is the appropriate level of access?
- Is access governance important to an organization's overall information security strategy and if so, why?
- What are the most frequently used approaches to assigning access rights?
- Who is accountable for governing access?
- How important is understanding risk relative to a user's role and the type of information resources they are accessing?
- What are the critical success factors in an access governance program?

A finding consistent in both studies is that IT staffs cannot keep up with the constant change to information resources, regulations and user access requirements. This lack of effective access governance jeopardizes organizations' ability to reduce the overhead and burden associated with achieving compliance, ensuring sustainable compliance with regulations and, as described above, mitigating access-related business risks.

The findings from this study illustrate a continuing lack of effective access governance processes that could expose organizations to risk. Respondents are reporting even greater difficulty with key access governance issues, such as poor management of access rights and keeping pace with access changes, when compared to the previous study.

Access governance ensures that users of information resources – which include applications, files and data – have no more or less rights to specific information resources than needed to do their particular job function within an organization. Access governance also helps ensure that end users' right to use or view business information resources does not violate compliance regulations as required by financial controls legislation, various data protection and privacy regulations, and industry mandates.[2]

---

[1]The first study was entitled, *2008 National Survey on Access Governance: US Study of IT Practitioners*, published February 2008.

[2]For example, Sarbanes-Oxley, Euro-SOX, CA 52-313, MAR, GLBA, PCI, HIPAA/HITECH, PIPEDA, MA CMR17, EU Data Protection Directive, Basel II, Solvency II, FFIEC, FERC/NERC, FISMA and others.

In addition to these general responsibilities, organizations must also deal with a difficult overall economic environment in which businesses are undergoing restructuring and must comply with new or more rigorous regulations. Business pressures are forcing IT organizations to make better use of their limited staff.

With all that in mind, some of the most important findings of this survey include:

- **User access rights continue to be poorly managed.** Eighty-seven percent of respondents believe that individuals have too much access to information resources that are not pertinent to their job description – up 9 percent from the 2008 study.

- **Organizations are not able to keep pace with changes to users' job responsibilities and they face serious noncompliance and business risk as a result.** Nearly three out of four organizations – 72 percent – say they cannot quickly respond to changes in employee access requirements and more than half (52 percent) cannot keep pace with the number of access change requests that come in on a regular basis.

- **Policies are not regularly checked and enforced.** Fifty-nine percent of organizations do not have or strictly enforce access governance policies and 61 percent do not immediately check access requests against security policies before the access is approved and assigned.

- **Organizations lack budget, resources and staff for effective access governance.** Nearly two-thirds (65 percent) say that not having enough IT staff was a key problem in enforcing access compliance policies. Fifty-seven percent of organizations do not have enough technologies to manage and govern end-user access to information resources and even more – 63 percent – do not have enough resources to do so.

- **Granting end-user access to information resources is increasingly seen as a responsibility for business units, not IT staff.** Nearly two out of five respondents – 37 percent – say business unit managers in their organizations are responsible for end-user access requests to information resources, up 8 percent from 2008. Conversely, information technology and security personnel saw their overall responsibility drop 2 percent to 23 percent in the 2010 study.

- **Cloud computing is expected to impact access governance processes.** Nearly three out of four (73 percent) respondents say that adoption of cloud-based applications will have a very significant or significant impact on business and end users ability to circumvent existing access policies.

- **Company data and applications are considered the most at risk from poor access governance**. From 2008 to 2010, respondents' concern grew most for business unit-specific applications (63 percent, up 11 percent), company intellectual property (57 percent, up 7 percent) and general business information (56 percent, up 11 percent).

II. Key Findings

Following are the most salient findings of this survey. Most of these findings will be shown in bar chart format. The actual data used in each figure and referenced in the paper will be shown in the percentage frequency tables attached as an appendix to this paper.

1. Organizations encounter obstacles in handling rapidly changing information resources and employee access requirements.

Pie Chart 1 illustrates that only 32 percent of respondents are very confident or confident that their organizations have enterprise-wide visibility for user access and can determine if that access is compliant with policies. The pie chart also shows that of the 34 percent of respondents who are not confident, their main reason (42 percent) is the inability to keep up with changes occurring with their organizations' information resources (on-boarding, off-boarding and outsourcing for management).

Pie Chart 1: How confident are you that your organization has enterprise-wide visibility for user access and can determine if it is compliant with policies.

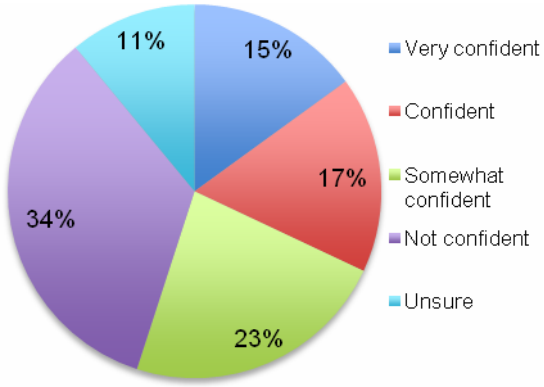


Table 1: If not confident, why?

We cannot create a unified view of user access across the enterprise.	25%
We only have visibility into user account information but not entitlement information.	21%
We cannot apply controls that need to span across information resources.	12%
We cannot keep up with the changes occurring to our organization's information resources.	42%

In this study, we asked IT practitioners their perceptions about access governance in their organization. Their responses suggest gaping holes in organizations' ability to ensure policies, processes and automation of key access governance tasks are adhered to:

- 63 percent believe there are not enough resources to manage and govern user access to information resources.
- 61 percent do not believe access requests are immediately checked against security policies before the access is approved and assigned.
- 59 percent believe there is not strict enforcement of access policies.
- 57 percent do not believe their organizations have enough technologies to manage and govern user access to information resources.

What's more, nearly three out of four organizations – 72 percent – say they cannot respond quickly to changes in employee access requirements and more than half (52 percent) cannot keep pace with the number of access change requests that come in on a regular basis. Dissatisfaction with this poor performance is evident in other telling statistics: 62 percent of respondents identify IT security as a bottleneck in the access delivery process and 48 percent say the process for business users to request access is too burdensome.

These complaints arise from the fact that the model most organizations use to control access requests (either for new access or a change to existing access) cannot keep up with today's fast-paced, ever-

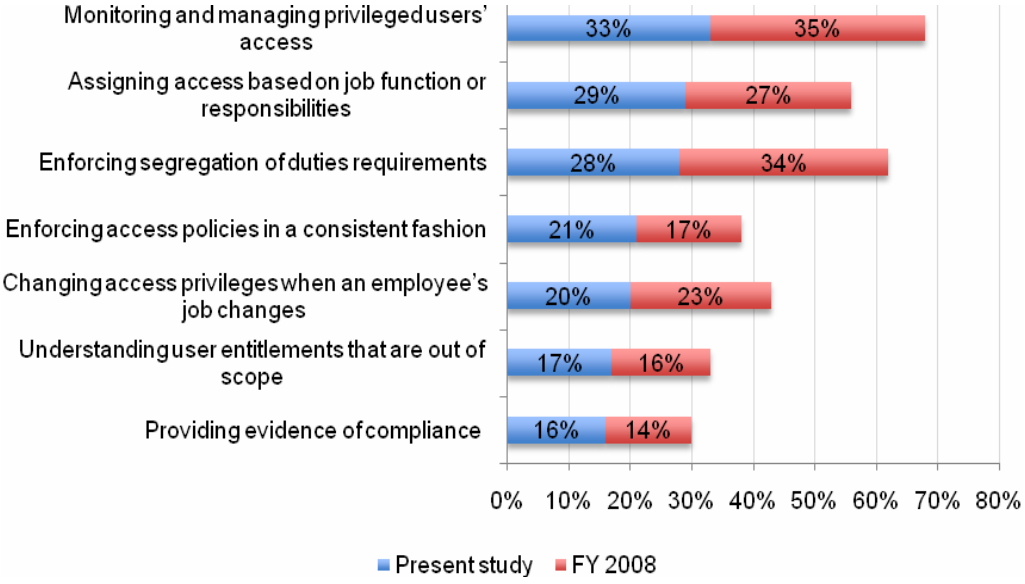
changing organizational environment. Access changes are occurring too rapidly and organizations have basically hit the wall. In trying to meet the needs of the business, organizations are circumventing the application of access control policies to ensure that the needs of the business are met. This can greatly increase organizations' security risks.

2. Organizations find it difficult to enforce common access governance tasks and policies.

We asked IT practitioners to tell us how well their organization can ensure that access polices for certain tasks are enforced. As shown in Bar Chart 1, 33 percent say they are excellent or good at monitoring or managing privileged users' access (system administration, root level access). However, this is down slightly (2 percent) from 2008. Twenty-nine percent say they are excellent or good at assigning access based on job function or responsibilities. This improved slightly (also 2 percent) from 2008.

Enforcing segregation of duties requirements declined to 28 percent from 34 percent in 2008 of respondents who believe they are excellent or good at this task. There was a slight improvement (4 percent) in enforcing access policies in a consistent fashion across all information resources in the organization.

Bar Chart 1
How well does your organization make sure policies for the following tasks are performed?
Each percentage reflects the excellent and good response combined (5-point scale)

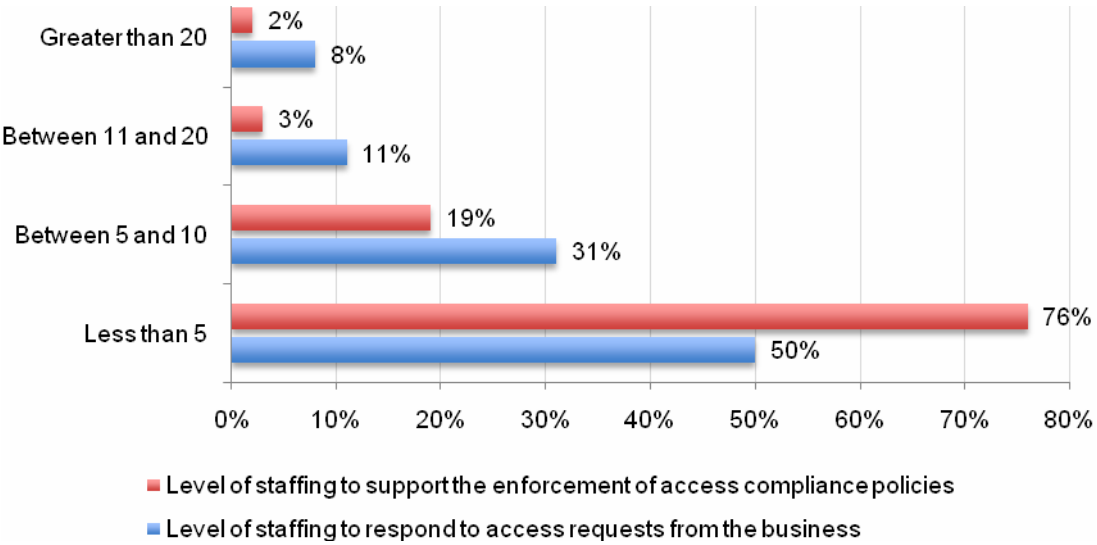


A major takeaway from these findings is that IT organizations need to improve their enforcement of basic tasks used to identify access change events or mechanisms to apply control at the point of access change. This is a huge issue considering the complexity of many organizations' access environments, in which they must manage hundreds or thousands of applications used by thousands – or tens of thousands or hundreds of thousands – of users.

3. Organizations lack sufficient staff to keep up with access governance requirements.

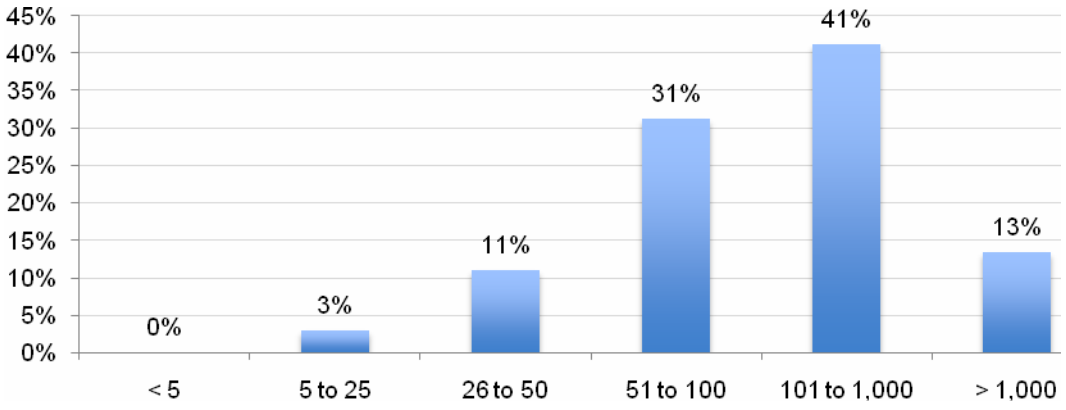
Bar Chart 2 shows that 81 percent of respondents have 10 or fewer employees responsible for access request support and 50 percent of respondents have fewer than five. More than three-quarters of respondents – 76 percent – have fewer than five employees responsible for enforcing and reporting on access compliance policies and 95 percent have no more than 10 employees in those roles.

Bar Chart 2
Level of staffing for responding to access requests and for enforcing access policies



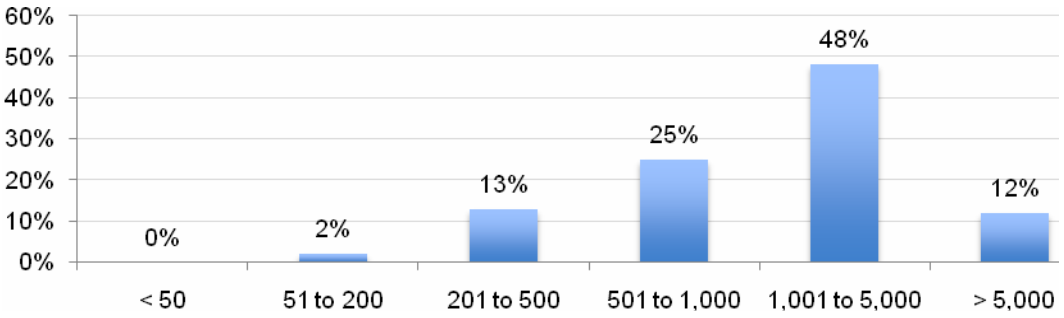
This small number of employees has daunting responsibilities. Bar Chart 3 shows that 87 percent of organizations have up to 1,000 information resources (applications, databases, etc.) that require the assignment of user access rights.

Bar Chart 3
Frequency of information resources that require the assignment of user access rights

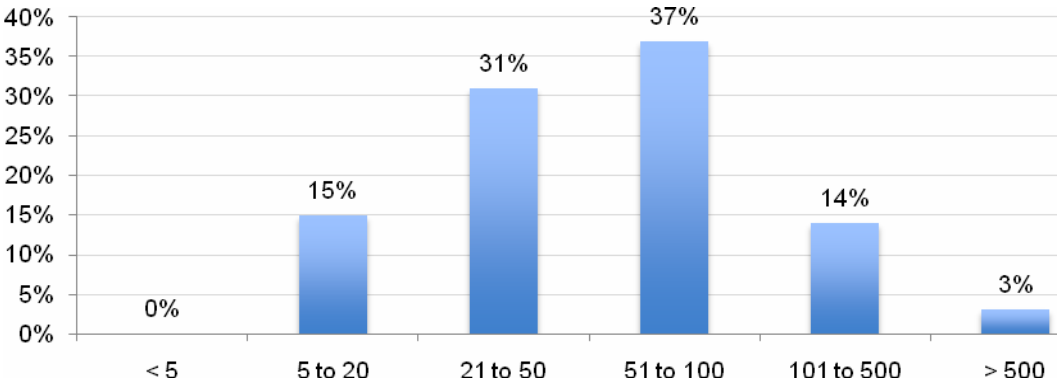


Bar Chart 4 shows that 73 percent of organizations have more than 500 access requests a month and 60 percent have more than 1,000 requests a month. Bar Chart 5 shows that 83 percent of organizations have up to 100 information resources that must comply with regulations or industry mandates such as the Payment Card Industry (PCI) standard, Sarbanes-Oxley legislation and HIPAA/HITECH requirements.

Bar Chart 4
Frequency of access requests made on a monthly basis

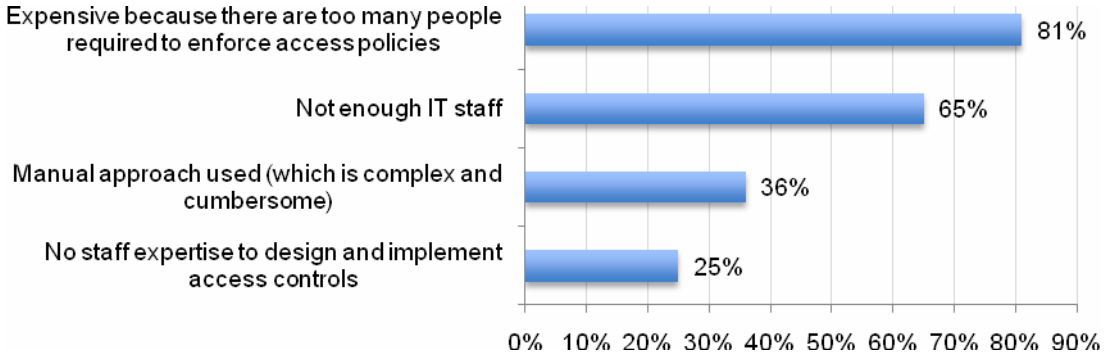


Bar Chart 5
Frequency of information resources that need to comply with regulations or industry mandates



Not surprisingly, Bar Chart 6 shows that nearly two-thirds (65 percent) say not having enough IT staff is a key problem in enforcing access compliance policies.

Bar Chart 6
The key problems enforcing access compliance policies



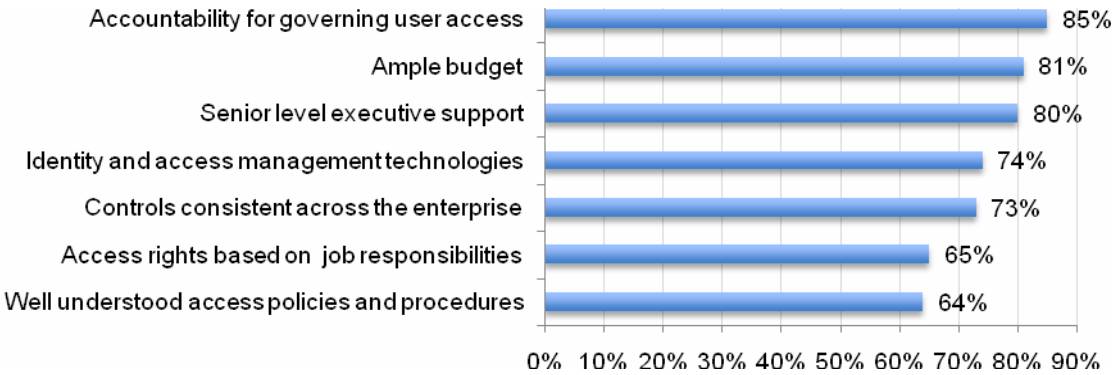
One possible reason for low staffing is that more than four out of five respondents (81 percent) indicate it requires too many people to enforce access policies, making the overhead to achieve compliance too expensive.

To date, organizations have tried to tackle the access governance problem with human capital. As the pace of change increases, and regulatory requirements and audits become more rigorous, additional staff is no longer an effective stopgap measure. With so few people to manage so many resources, requests and control requirements, many companies are at risk that users may be accessing information they should not.

4. Accountability, budget and senior executive support are the most critical success factors.

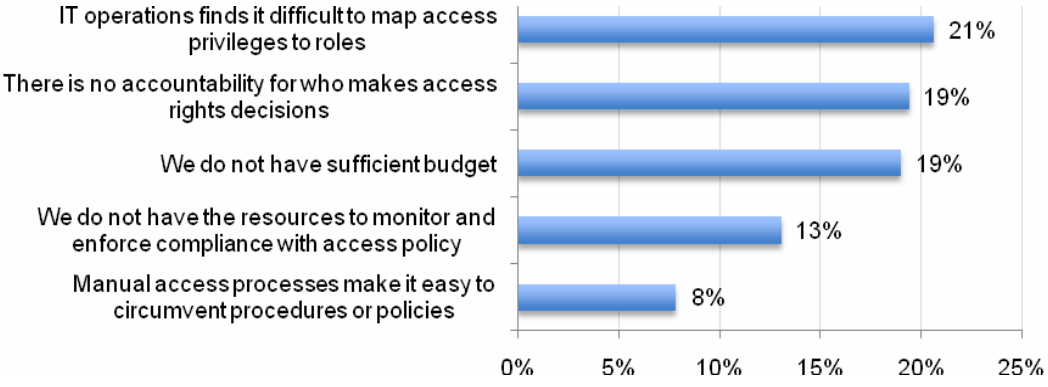
Bar Chart 7 shows that 85 percent of respondents say accountability for governing user access owned by the business is a critical success factor for implementing access governance across the enterprise, followed by ample budget (81 percent) and senior level executive support (80 percent). Respondents have a greater appreciation for well-understood access policies and procedures, which rose 12 percent from 2008 (52 to 64 percent this year).

Bar Chart 7
Critical success factors for implementing access governance across the enterprise



Conversely, Bar Chart 8 shows when implementing access governance across the enterprise, IT operations finds it difficult to map access privileges to roles (21 percent), followed closely by a lack of accountability for who makes access rights decisions and a lack of sufficient budget (both at 19 percent).

Bar Chart 8
Key problems when implementing access governance across the enterprise



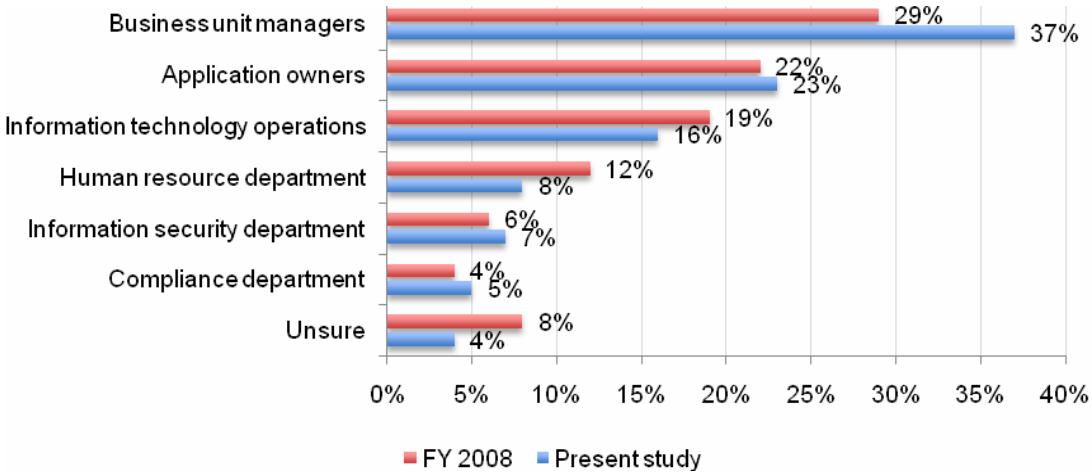
These findings suggest a lack of precise access privileges, accountability, and insufficient budgets can have a negative impact on achieving access governance. Taking this one step further, the business may be unable to understand the raw technical access rights IT puts in front of them. This gap creates potentially serious issues for compliance and risk management, such as inefficiency in granting or

certifying access requests. Misunderstandings between business and IT often results in serious time delays and backlog in assigning access rights.

5. Senior management wants IT staff to oversee access governance but business units are often in charge of those responsibilities.

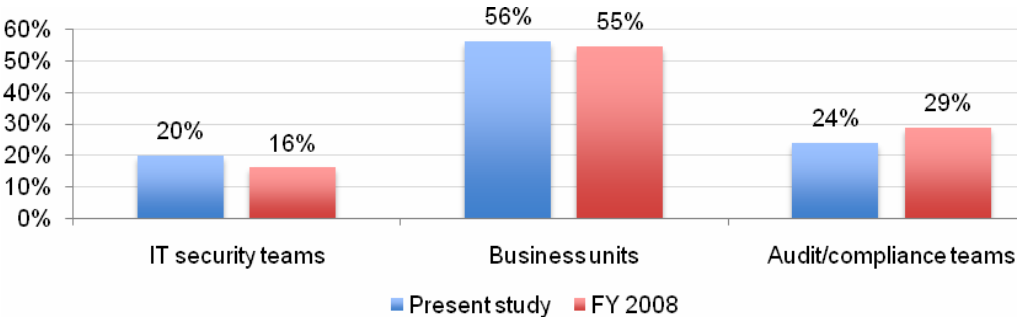
In this study, 49 percent of respondents say their senior leadership prefers IT operations to manage and control access privileges for the enterprise, while 43 percent say their senior leadership prefers each business unit to make those decisions. Granting end-user access to information resources is increasingly seen as a responsibility for business units, not IT staff. Bar Chart 9 shows that nearly two out of five respondents – 37 percent – say business unit managers in their organizations are responsible for end-user access requests, up 8 percent from 29 percent in 2008. Conversely, information technology and security personnel saw their overall responsibility decline, from 25 percent in 2008 to 23 percent in 2010.

Bar Chart 9
Who is responsible for making the decision for granting end-user access



Bar Chart 10 shows that by a more than 2-1 margin, business units are responsible for conducting user access certification. More than half of respondents (56 percent) say business units control that function, compared to only 20 percent who say IT security teams play that role. Both business units and IT security teams saw increased responsibility while fewer organizations relied on audit/compliance teams for those functions – only 24 percent, from 29 percent in 2008.

Bar Chart 10
Most responsible for conducting user or role certification



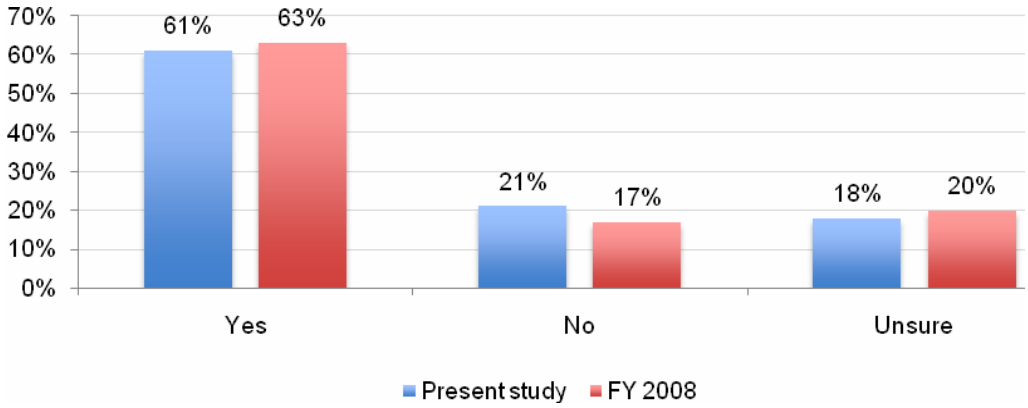
The lack of a majority opinion on which group should manage access governance could indicate confusion about who should be accountable for what aspects of governance. The findings also suggest

organizations must encourage collaboration among IT security, business and internal audit/compliance groups to help ensure effective access governance. Teamwork is critical because each party has invaluable knowledge and experience the others do not. The business understands what access is necessary for a functional job role and is ultimately responsible for vetting decisions. Internal audit/compliance defines proper controls that demonstrate regulatory compliance, while IT security facilitates the process and manages risks through the automation of controls.

6. More organizations are judging end users' access to information based on job function but fear employees have more access than they need.

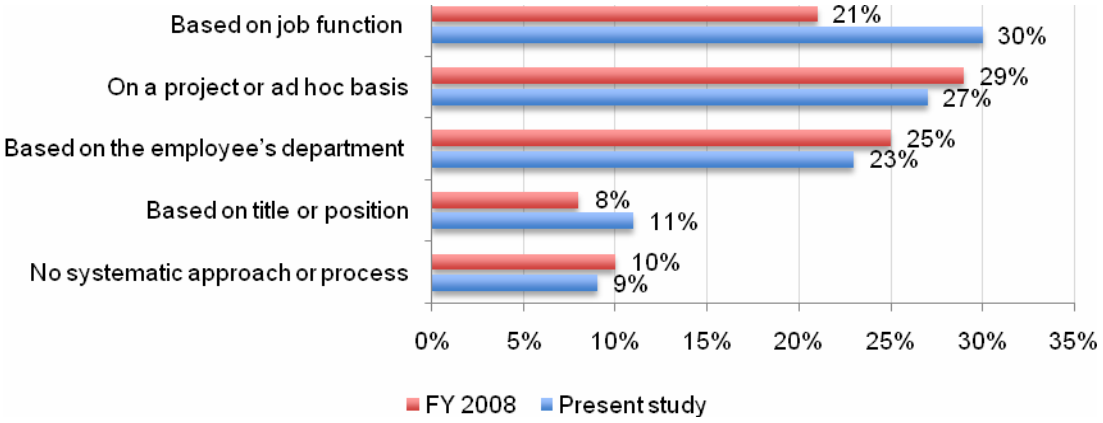
Bar Chart 11 shows 61 percent of respondents say their organizations determine user access rights by a user's clearance to highly sensitive information resources, down slightly from 2008. More respondents know whether their organizations did not use that criterion – 21 percent, up from 17 percent. Fewer are unsure – 18 percent, down from 20 percent.

Bar Chart 11
Are user access rights determined by clearances to highly sensitive information



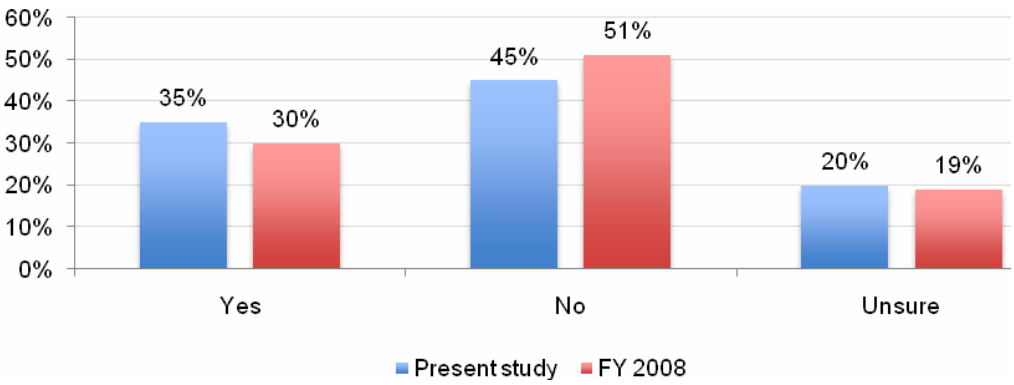
resource
In Bar Chart 12, more organizations are granting end users access to information based on job function – 30 percent, up from 21 percent in 2008.

Bar Chart 12
How is access to information resources granted to end-users?



Bar Chart 13 shows more organizations are validating or checking changes to access status but most still do not or are unsure if they do. Thirty-five percent of respondents say they performed such checks, up 5 percent from 30 percent in 2008. Fewer respondents do not check – 45 percent, down 6 percent from 51 percent last year – and slightly more are unsure.

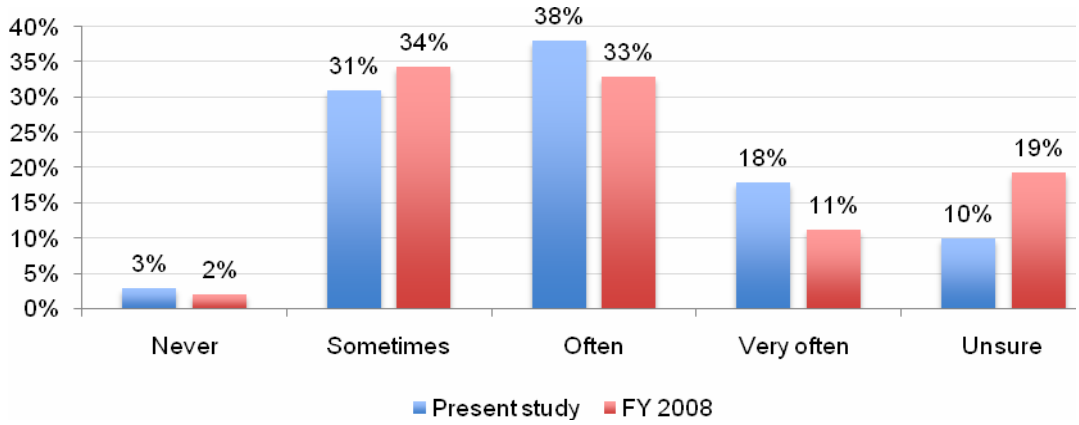
Bar Chart 13
Are changes to access validated or checked?



These findings suggest many companies have great difficulty ensuring the accuracy of delivery of the access change process. They must ensure appropriate user access and then mitigate risk when they revoke that access; however, they have no way to determine if access is appropriate for people as they transfer into new business units, locations or functional responsibilities . This lack of visibility raises the strong possibility of users retaining access rights they do not need or receiving too much or too little access. It could also create security risks, such as orphan (inactive user) accounts vulnerable to exploitation by both internal and external malicious attackers.

This lack of transparency has led more organizations to report that many of their users have more access than is required to do their jobs – and the problem is getting worse. Bar Chart 14 shows 56 percent of respondents say end users often or very often have more access than required, up 12 percent from 44 percent in 2008.

Bar Chart 14
How likely would end-users in your organization have more access than is required for their job?



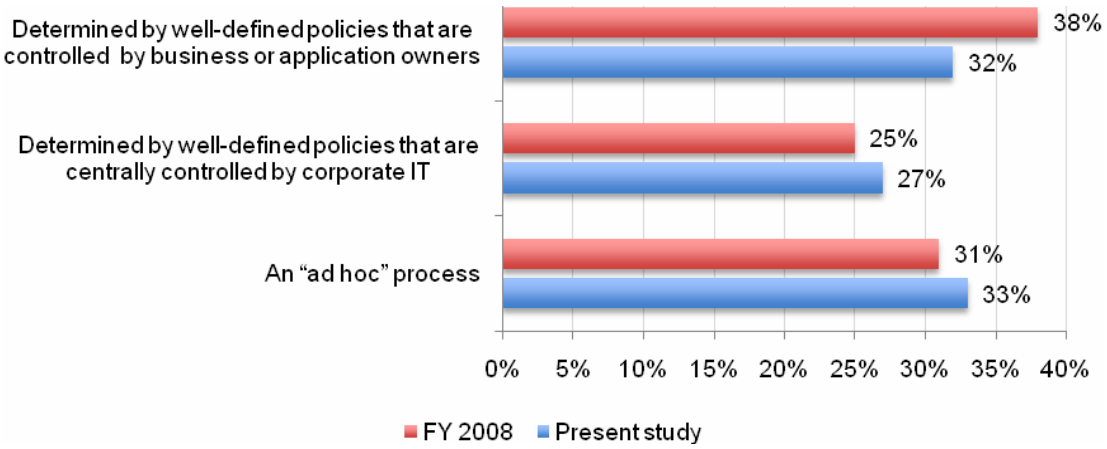
On a positive note, the percentage of organizations that are unsure whether users have too much access dropped nearly by half, from 19 percent to 10 percent.

Many organizations lack a framework or process for access change management that can accommodate continuous changes to user relationships and map those changes to a, complex and dynamic infrastructure. These findings suggest large numbers of individuals may be accessing information resources not in alignment with their job functions.

7. Most organizations rely on ad hoc or manual processes for key access governance activities.

Bar Chart 15 shows a roughly three-way split among ad hoc processes (33 percent), well-defined policies controlled by business units (32 percent) and well-defined policies centrally controlled by corporate IT (27 percent). This indicates a noticeable shift away from business units (down 6 percent from 38 percent in 2008) and slightly more toward ad hoc processes and corporate IT (up from 31 percent and 25 percent in 2008, respectively).

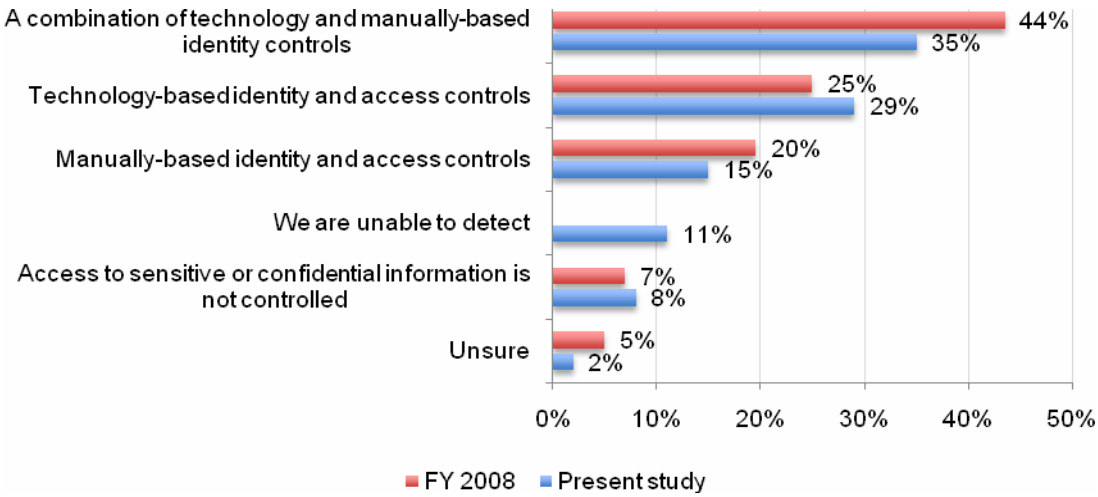
Bar Chart 15
What best describes the process for assigning access in your organization



Taken together, our findings indicate that the distributed nature of many organizations continues to cause breakdowns in centralized policy administration. Application owners are distributed throughout the organizations, which can contribute to the problem of ensuring proper access governance. The ad hoc approach described above can contribute to excessive user access and greatly decreases the ability to apply policies and processes consistently across the enterprise. If access is granted based on a time period or project, organizations need processes in place to ensure that entitlements are revoked when no longer needed.

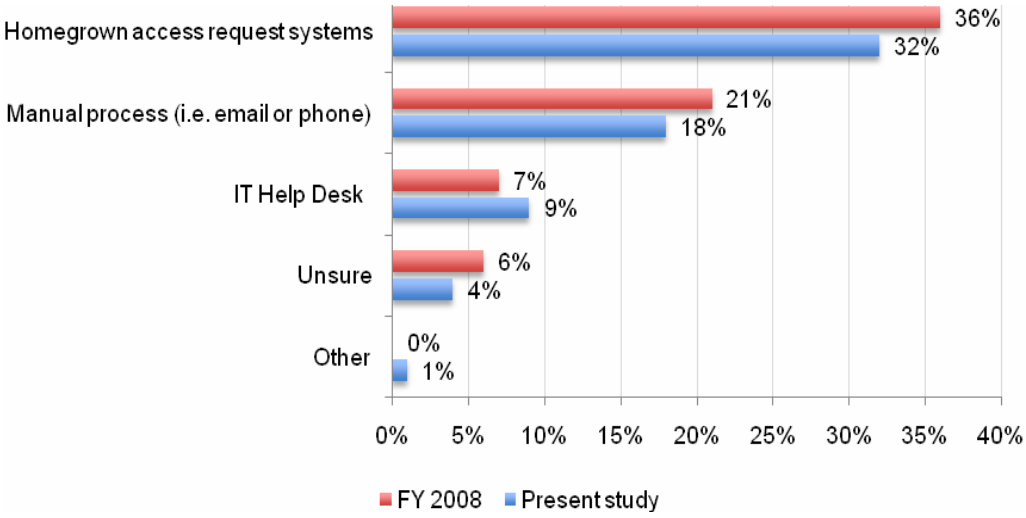
Organizations are also using more technology-based solutions to monitor and manage privileged users. As shown in Bar Chart 16, organizations still prefer a combination of technology and manual identity and access controls (35 percent) to detect privileged users' systems administration and root level access rights. More respondents appear to prefer technology solutions (29 percent, up 4 percent) and are less likely to use only manual controls (15 percent, down 5 percent). Eleven percent of respondents say they cannot detect privileged users' access rights at all.

Bar Chart 16
How do you detect the sharing of system administration access or root level access rights?



Bar Chart 17 shows more organizations are relying on commercial off-the-shelf (COTS) automated solutions to assist with access governance. Use of COTS rose 6 percent, from 30 percent in 2008 to 36 percent this year. Homegrown access request systems continues to be a favorite at 32 percent, down 4 percent from 2008. This data suggests more organizations are realizing automated technology solutions are a key tool to ensure employees' access requests are validated, monitored and do not pose security risks.

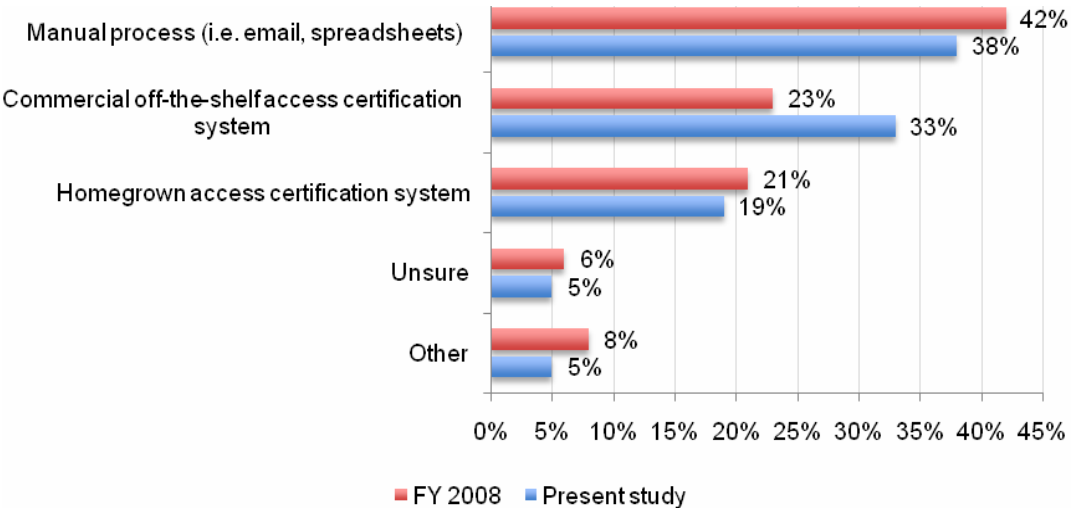
Bar Chart 17
What processes are used for granting user access to information resources?



Bar Chart 18 shows that although COTS products grew in popularity to review and certify user access, rising 10 percent to 33 percent, manual processes remain the most popular means to review and certify user access (38 percent, down from 42 percent). These findings suggest IT practitioners believe manual processes are becoming outdated and that COTS technologies are essential in the current access governance environment. As organizations mature their compliance processes, they are adopting COTS

to help ensure those processes are more auditable, repeatable and sustainable. Consequently, the purchase of such technologies requires sufficient financial resources and senior executive buy-in.

Bar Chart 18
What processes are used to review and certify user access?

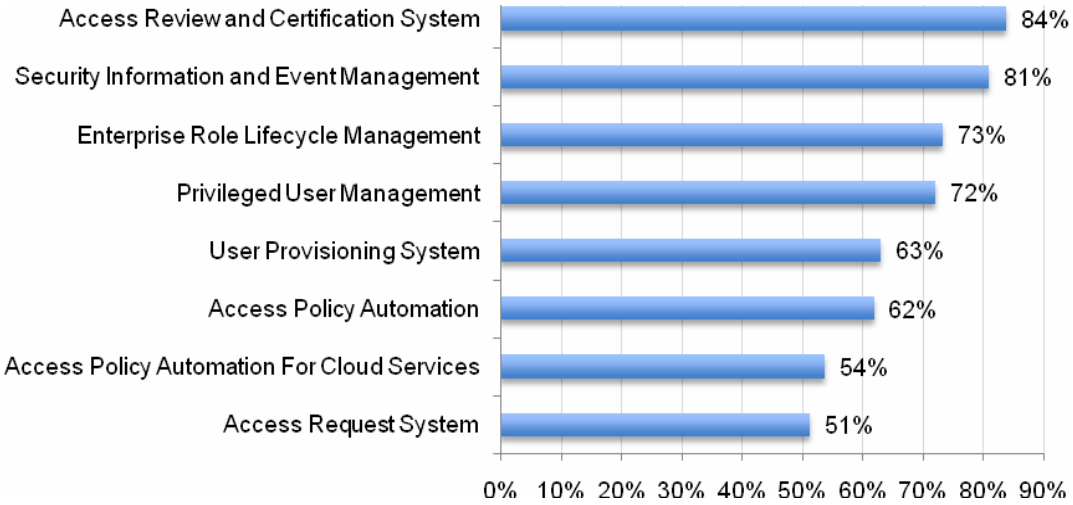


This data supports the observation that organizations are turning increasingly to readily available automated solutions to help overtaxed IT staff meet growing access governance needs. Organizations that do not move to COTS solutions face a greater compliance burden through manual processes, which are often weak, error-prone and not an auditable system of record.

8. The identity and access management technologies most often implement are not in sync with current access governance needs.

The most commonly implemented identity and access management technologies are homegrown access request systems (80 percent), user provisioning systems (74 percent) and security information and event management (SIEM) systems (56 percent).

Bar Chart 19
The identity and access management technologies most important for achieving security



As shown in Bar Chart 19 (above), the most effective enabling technologies are access review and certification systems (83 percent), SIEM systems (81 percent) and enterprise role lifecycle management systems (73 percent).

Even though only 43 percent of respondents have implemented access review and certification systems, 83 percent say that was an important technology. An even wider gap exists with enterprise role lifecycle management systems, which only 32 percent of respondents have implemented.

A disconnect exists between the technologies organizations have and the technologies they would prefer to use for access control. A possible explanation is that widely implemented identity management technologies, and in particular user provisioning**,** are unable to address current access governance needs.

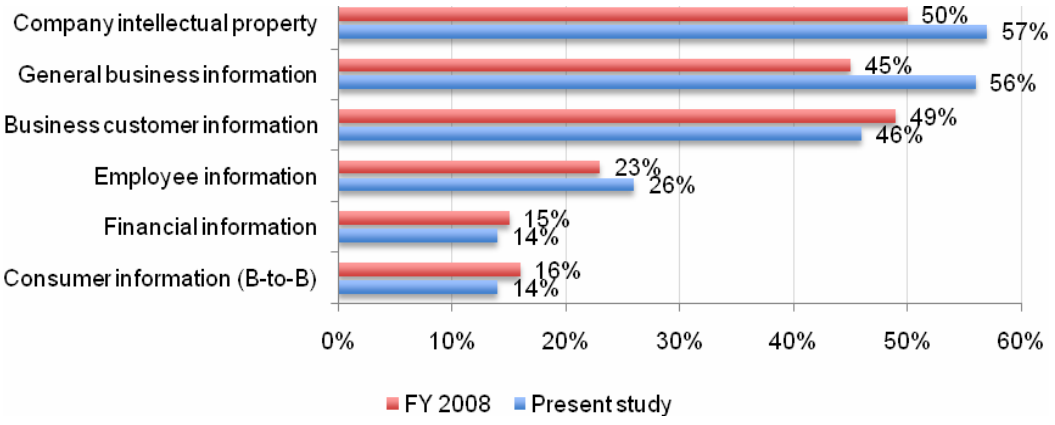
This finding suggest that because access is a core part of compliance mandates, IT security organizations' ability to streamline access authorization and certification through appropriate access rights management technologies may help reduce non-compliance risk. However, many organizations deploy homegrown access request systems designed to serve their core business but often cannot apply policy controls at the point of the access request. This weakness forces and organization into a detective compliance posture and can introduce business risks without the organization even realizing it.

Another implication is that organizations are struggling to define and embrace roles. This might be due to a language barrier on how access is expressed. Organizations that cannot express access so that it is meaningful for both IT security and the business will never be able to use roles. If organizations want business units to be accountable for user access, access policies and processes must be in a language those business units understand. IT security staffs, therefore, must translate technical roles and entitlements into business terms.

9. Business-oriented data and applications are considered the most at risk from poor access governance.

Bar Chart 20 shows respondents consider company intellectual property (57 percent, up 7 percent from 50 percent in 2008) and general business information (56 percent, up 11 percent from 45 percent in 2008) to be the data types that poor access governance puts most at risk. Customer information came in a solid third at 46 percent, down 3 percent from 49 percent in 2008.

Bar Chart 20
Data most at risk because of a lack of proper access controls



The business unit-specific applications are considered the most at risk from poor access governance – at 63 percent the clear leader, rising 11 percent from 52 percent in 2008. New for this year, cloud-based applications took the number-two spot with 40 percent, which was not surprising given other results in the

survey. Revenue-generating applications (30 percent, up slightly from 29 percent last year) and CRM applications (29 percent, down 7 percent from 36 percent in 2008) were nearly tied for third place.

The fact that business data and applications led their respective categories and increased sharply from the 2008 study suggests many organizations assign access governance responsibilities to business units rather than IT. This also may explain why there is a small increase in concern for revenue-generating applications.

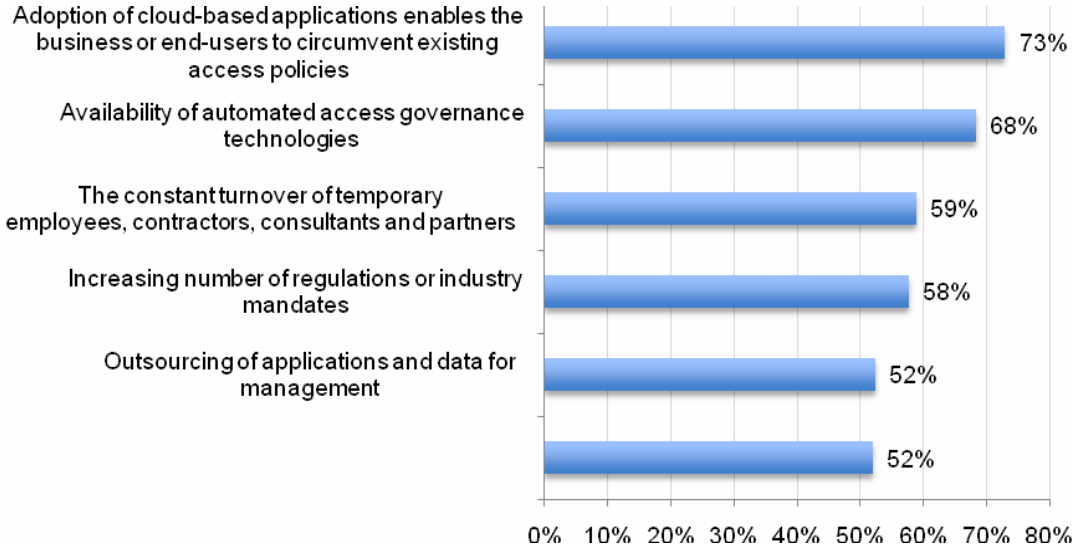
CRM and other revenue-generating applications typically contain significant amounts of confidential customer data for use by call center operations, marketing and sale force activities. Failing to control access to these types of applications may exacerbate insider risk.

The decreased concern for the safeguarding of financial information may be due to the fact that compliance mandates such as Sarbanes-Oxley may be successful in meeting their objectives. An area that organizations may want to become more vigilant concerns the plethora of non-financial business information such as corporate intellectual properties.

10. Cloud computing and automated technologies affect access governance processes.

Bar Chart 21 shows that nearly three out of four (73 percent) of respondents say the adoption of cloud-based applications enables business and end users to circumvent existing access policies. Nearly as many (68 percent) say the availability of automated access governance technologies would affect their organizations' access governance process.

Bar Chart 21
Attributions about the state of access governance in respondents' organizations



Other key factors that would affect access governance processes are constant turnover of non-permanent employees such as contractors (59 percent), an increasing number of regulations or industry mandates (58 percent), outsourcing of applications and data for management (52 percent) and organizational restructuring (also 52 percent).

Taken together, these findings suggest that today's dynamic business environment coupled with changing technologies make it more difficult to achieve access governance. Clearly, effective access management is essential to mitigate risk, especially an increasingly popular cloud computing environments. As adoption of cloud-based applications and services are often purchased directly by

business units without consideration for access governance, could raise administrative and deployment problems.

The growing popularity of IT outsourcing raises numerous challenges for organizations that want to extend access governance policies beyond their firewalls into the cloud, especially for outsourcing data management and outsourced services. The challenge is to know not only what they let onto their systems but what they're putting outside their networks and where. They must prevent users from bypassing security controls and ensure cloud service providers offer proper security.

III: Methods

A sampling frame of more than 12,000 adult-aged individuals who reside within the United States was used to recruit and select participants to this survey. Our randomly selected sampling frame was built from several proprietary lists of experienced IT and IT security practitioners.

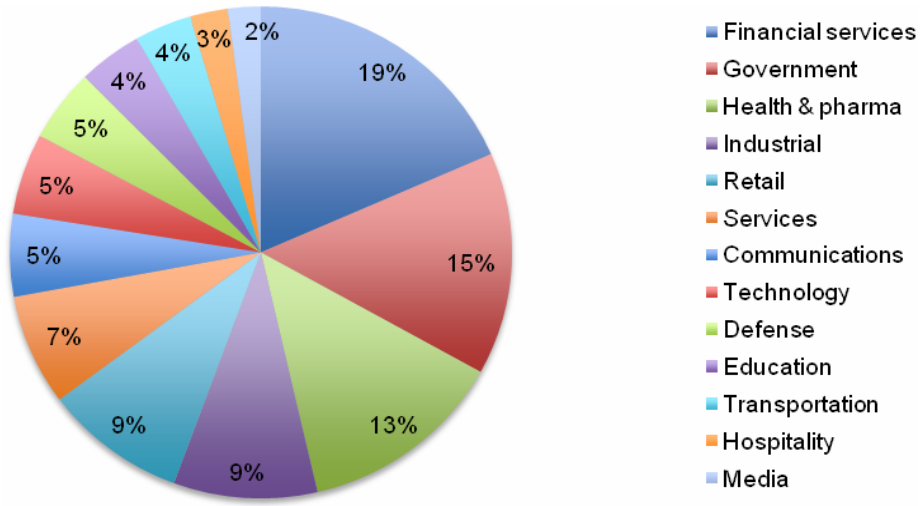
Table 2: Sample response statistics	Freq.	Pct%
Sampling frame	12091	100.0%
Invitations	10995	90.9%
Bounce back	1863	15.4%
Total response	796	6.6%
Rejections	68	0.6%
Final sample	728	6.0%

In total, 796 respondents completed the survey. Of the returned instruments, 68 surveys failed reliability checks. A total of 728 surveys were used as our final sample, which represents a 6.0 percent response rate.

Two screening questions were used to ensure respondents had relevant knowledge and experience, resulting in a reduced sample size of 641 individuals. Ninety percent of respondents completed all survey items within 17 minutes.[3] The average overall experience level of respondents is 10.3 years, and the years of experience in their present job is 4.6 years.

Pie Chart 2 reports the primary industry sector of respondents' organizations. As shown, the largest segments include financial services, government, pharmaceuticals and healthcare (combined), industrial and services.

Pie Chart 2: Industry distribution of respondents' organizations



[3] Please note that nominal compensation was provided to respondents who successfully completed the survey instrument.

Table 3 reports the respondent organization's global headcount. As shown, a majority of respondents work within companies with more than 5,000 employees. Over 29 percent of respondents are located in larger-sized companies with more than 25,000 employees.

Table 3: The worldwide headcount of respondents' organizations	Pct%
Less than 500	7%
500 to 1,000	9%
1,001 to 5,000	25%
5,001 to 25,000	30%
25,001 to 75,000	17%
75,001 to 100,000	6%
101,000 to 150,000	3%
More than 150,000	3%

Table 4 reports the respondent's primary reporting channel. As can be seen, 56 percent of respondents are located in the organization's IT department (led by the company's CIO). Nineteen percent report to the company's security officer (or CISO).

Table 4: Respondent's primary reporting channel	Pct%
CEO/Executive Committee	0%
Chief Financial Officer	3%
General Counsel	0%
Chief Information Officer	56%
Compliance Officer	5%
Human Resources VP	5%
Chief Security Officer	4%
Chief Information Security Officer	19%
Chief Risk Officer	6%
Other	2%

Table 5 reports the respondent organization's global footprint. As can be seen, a large number of participating organizations are multinational companies that operate outside the United States, Canada and Europe.

Table 5: Geographic footprint of respondents' organizations	Pct%
United States	100%
Canada	63%
Europe	65%
Middle east	12%
Asia-Pacific	40%
Latin America	39%

IV. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

V: Implications & Recommendations

Our findings suggest that IT staffs cannot keep up with the constant change to information resources, regulations and user access requirements. Many organizations are facing significant information risks because of a lack of resources, budget and IT staff, as well as ad hoc or inconsistent approaches to access management activities across the enterprise.

Many organizations emphasize certification in their access governance processes. This "check-in-the-box" mindset does not address a wide-array of security threats. Organizations' IT staff may not be proactive in discovering access-related problems. This complacency increases the risk of inappropriate or illegal access rights and privileges.

We believe this study shows the need for organizations to address the insider risk caused by inappropriate access governance processes. We recommend that they consider implementing preventative and detective controls that span both access request and access certification. A continuous approach for access governance, and not just periodic or reactive assessment, will enable leading organizations to decrease their compliance burden and the threat of insider malfeasance or negligence.

IT practitioners surveyed generally see the need for a strategic, unified approach to access governance and related responsible information management practices. Some specific recommendations based on the findings of this survey include:

- Implement a well-managed enterprise-wide access governance process that keeps employees, temporary employees and contractors from having too much access to information assets. At the same time, do not hinder individuals' access to information resources critical to their productivity. To do this, organizations must understand what role-based access individuals need. Further, changes to users' roles must be managed to ensure they have current and correct access rights.

- Create well-defined business policies for the assignment of access rights. These policies should be centrally controlled to ensure they are enforced in a consistent fashion across the enterprise. They also should encourage collaboration among different internal groups.

- Understand how to make the case for building enterprise-wide access governance to senior management. Factors to include are the fines and penalties for noncompliance and downtime as a result of negligence. With respect to data breaches, emphasize how they can impact an organization's bottom line.

- Track and measure the ability to enforce user access policies. This includes measuring the effectiveness of processes to manage changes to users' roles; revoking access rights upon an individual's termination; monitoring access rights of privileged users' accounts; and monitoring segregation of duties.

- Ensure that accountability for access rights is assigned to the business unit that has domain knowledge of the users' role and responsibility.

- Become proactive in managing access rights. Instead of making decisions on an ad hoc basis based on decentralized procedures, build a process that enables the organization to have continuous visibility into all user access across all information resources and entitlements to those resources. Technologies that automate access authorization, review and certification will limit the risk of human error and negligence.

- Bridge the language gap between IT staff and business managers to encourage a common understanding of how to express access rights and entitlements. This is especially important for the access request and access certification processes, in which gaps can cause unnecessary delays in access delivery or allows inappropriate access.

- Pursue extending controls over access to all information resources similar to those required under regulations (SOX, PCI, etc). This entails organizations broadening their view of risk management beyond compliance with specific regulations. Organizations need to go beyond the minimum requirements for compliance and think about risk in the broadest terms with the widest coverage. This is especially true because the loss of corporate IP is typically not covered under regulations or industry mandates.

- Extend the organizational access governance framework beyond the firewall to cloud computing and other IT outsourcing/software-as-a-service (SaaS) providers.

Appendix I: Survey Details

Sample response	Freq.	Pct%
Sampling frame	12,091	100.0%
Invitations	10,995	90.9%
Bounce back	1,863	15.4%
Total response	796	6.6%
Rejections	68	0.6%
Final sample	728	6.0%

I. Screening		
Q1. What best describes your level of involvement in providing end-users access to information resources in your organization?	Freq.	Remainder
None	12	0
Low	29	0
Moderate	83	83
Significant	339	339
Very significant	265	265
Total	728	687

Q2. What best describes your role in providing end-users access to information resources in your organization? Please check all that apply.	Freq.	Subtract
Respond to access requests	458	
Support the delivery of access	631	
Support the enforcement of access policies	600	
Responsible for review and certification of access compliance	447	
Install technologies relating to access rights management	389	
Other	16	
None of the above	87	87
Total	2628	641

II. Attributions. Please rate your opinion for Q3a to Q3h using the scale provided below each statement.	Strongly agree	Agree
Q3a. In my organization, access governance policies are in-place and are strictly enforced.	14%	27%
Q3b. In my organization, we have **enough technologies** to manage and govern end-user access to information resources.	13%	30%
Q3c. In my organization, we have the **necessary resources** to manage and govern end-user access to information resources.	13%	24%
Q3d. In my organization, the function responsible for providing end-users with access to information resources is quick to respond to changes in our business such as on-boarding access when employees join the organization or changing access when an employee transfers within the organization or in the event of mergers/acquisitions, divestures, reorganizations and workforce reductions.	10%	18%
Q3e. In my organization, senior leadership prefers IT operations to manage and control access privileges for the enterprise.	20%	29%
Q3f. In my organization, senior leadership prefers each business function to determine what access privileges are required for a user's role and function.	20%	23%

Q3g. In my organization, IT security is viewed as a bottleneck in the access delivery process.	30%	32%
Q3h. In my organization when a request for access is made, the request is immediately checked against security policies before the access is approved and assigned.	11%	28%

III. Current access governance practices

Q4. Please review all 8 identity & access management technologies below that may be used in your organization (by placing an X in the Yes column). Then, for each item selected, indicate the relative importance of the technology with respect to achieving your organization's security goals or mission.

Identity & Access Management Technologies	Yes
Enterprise Role Lifecycle Management	32%
Access Request System	80%
Access Policy Automation	50%
Access Review and Certification System	43%
Privileged User Management	39%
Security Information and Event Management	56%
Access Policy Automation For Cloud Services	12%
User Provisioning System	74%

Identity & Access Management Technologies	Very important	Important
Enterprise Role Lifecycle Management	47%	26%
Access Request System	16%	36%
Access Policy Automation	38%	24%
Access Review and Certification System	52%	31%
Privileged User Management	50%	22%
Security Information and Event Management	51%	30%
Access Policy Automation For Cloud Services	26%	28%
User Provisioning System	27%	36%

Q5a. What level of staffing do you have to respond to access requests from the business and to support the fulfillment/delivery of access?	Pct%	Extrapolated value
Less than 5	50%	2
Between 5 and 10	31%	2
Between 11 and 20	11%	2
Greater than 20	8%	2
Total	100%	8

Q5b. What level of staffing do you have to support the enforcement of and reporting on access compliance policies?	Pct%	Extrapolated value
Less than 5	76%	3
Between 5 and 10	19%	1
Between 11 and 20	3%	0
Greater than 20	2%	0
Total	100%	5

Q6a. Approximately, how many information resources (applications, databases, networks, servers, hosts, file shares) within your organization require the assignment of user access rights?	Pct%	Extrapolated value
Less than 5	0%	-
Between 5 and 25	3%	0
Between 26 and 50	11%	4
Between 51 and 100	31%	23
Between 101 and 1,000	41%	206
More than 1,000	13%	162
Total	100%	396

Q6b. On a monthly basis, how many access requests are made (i.e. requesting new access, changes to existing access rights or revocation of access due to termination)?	Pct%	Extrapolated value
Less than 50	0%	-
Between 51 and 200	2%	3
Between 201 and 500	13%	45
Between 501 and 1,000	25%	188
Between 1001 and 5,000	48%	1,206
More than 5,000	12%	716
Total per month	100%	2,157
Total per year		25,890

Q6c. How many information resources in your organization need to be in compliance with regulations or industry mandates (e.g. PCI, FERC/NERC, SOX, GLBA, FISMA, ITAR, MAR, HIPAA/HITECH, FFIEC, BASEL II, State & Country-based privacy regulations, etc.)?	Pct%	Extrapolated value
Less than 5	0%	-
Between 5 and 20	15%	2
Between 21 and 50	31%	11
Between 51 and 100	37%	28
Between 101 and 500	14%	42
More than 500	3%	18
Total	100%	100

Q7. Are user access rights determined by a user's clearance to highly sensitive information resources?	Pct%	Q5a last year
Yes	61%	63%
No	21%	17%
Unsure	18%	20%
Total	100%	100%

Q8a. What types of data do you consider to be most at risk in your organization due to the lack of proper access control?	Pct%	Q6 last year
Customer information (B-to-B)	46%	49%
Consumer information (B-to-B)	14%	16%
Employee information	26%	23%
Financial information	14%	15%
General business information	56%	45%
Company intellectual property	57%	50%

Q8b. What type of applications do you consider to be most at risk in your organization due to the lack of proper access control? (Please select the top three)	Pct%	Q7 last year
Finance/ERP applications	15%	16%
CRM applications	29%	36%
Supply chain management applications	8%	9%
Revenue generating applications	30%	29%
Business unit specific applications	63%	52%
Productivity applications	10%	12%
Knowledge applications	14%	18%
Cloud-based applications (i.e. Salesforce.com)	40%	Not rated

Q9. What best describes the process for assigning access to information resources in your organization today? Please select one best choice.	Pct%	Q8 last year
An “ad hoc” process	33%	31%
Determined by well-defined policies that are centrally controlled by corporate IT	27%	25%
Determined by well-defined policies that are controlled by business or application owners	32%	38%
Unsure	8%	6%
Total	100%	100%

Q10. How likely would it be that end-users in your organization have more access than is required to do their job?	Pct%	Q9 last year
Never	3%	2%
Sometimes	31%	34%
Often	38%	33%
Very often	18%	11%
Unsure	10%	19%
Total	100%	100%

Q11. How is access to information resources granted to end-users?	Pct%	Q10 last year
On a project or ad hoc basis	27%	29%
Based on title or position	11%	8%
Based on job function	30%	21%
Based on the employee’s department	23%	25%
No systematic approach or process for granting access rights exist	9%	10%
Other	Not rated	7%
Total	100%	100%

Q12. Who is responsible for making the decision to grant an end-user access to information resources?	Pct%	Q11 last year
Information technology operations	16%	19%
Information security department	7%	6%
Compliance department	5%	4%
Business unit managers	37%	29%
Application owners	23%	22%
Human resource department	8%	12%
Unsure	4%	8%
Total	100%	100%

Q13a. What processes are used for granting user access to information resources. Please select the top two	Pct%	Q12 last year
Manual process (i.e. email or phone)	18%	21%
Homegrown access request systems	32%	36%
Commercial off- the-shelf automated solutions	36%	30%
IT Help Desk	9%	7%
Unsure	4%	6%
Other	1%	0%
Total	100%	100%

Q13b. What processes are used to review and certify user access? (Please select the top two)	Pct%	Q13 last year
Manual process (i.e. email, spreadsheets)	38%	42%
Homegrown access certification system	19%	21%
Commercial off-the-shelf access certification system	33%	23%
Unsure	5%	6%
Other	5%	8%
Total	100%	100%

Q14a. Does your organization use job or functional roles to make the determination for what access is appropriate?	Pct%	Q14a last year
Yes	58%	54%
No	42%	46%
Total	100%	100%

Q14b. If yes, is there a regular process to review the definitions of these roles and who has them?	Pct%	Q14b last year
Yes	50%	49%
No	50%	51%
Total	100%	100%

Q15. Who is responsible for conducting user or role certification?	Pct%	Q14c last year
IT security teams	20%	16%
Business units	56%	55%
Audit/compliance teams	24%	29%
Other	0%	1%
Total	100%	100%

Q16. Are changes to access validated or checked?	Pct%	Q17 last year
Yes	35%	30%
No	45%	51%
Unsure	20%	19%
Total	100%	100%

Q17. How do you detect the sharing of system administration access rights or root level access rights by privileged users? (Please select the top two)	Pct%	Q20 last year
Technology-based identity and access controls	29%	25%
Manually-based identity and access controls	15%	20%
A combination of technology and manually-based identity and access controls	35%	44%
Access to sensitive or confidential information is not really controlled	8%	7%
Unsure	2%	5%
We are unable to detect	11%	Not rated
Total	100%	100%

Q18. How well does your organization make sure access policies for the following tasks are enforced? Please use the following scale to rate each task provided using the 1 = excellent, 2 = good, 3 = fair, 4 = poor, 9 = task is not performed.	1 & 2 combined	Q21 last year
Assigning access based on job function or responsibilities	29%	27%
Revoking or changing access privileges as needed when an employee's job or function changes or their relationship with the organization is terminated	20%	23%
Enforcing access policies in a consistent fashion across all information resources in the organization	21%	17%
Monitoring and managing privileged users' access (system administration, root level access)	33%	35%
Enforcing segregation of duties requirements	28%	34%
Providing evidence of compliance with regulations and industry mandates	16%	14%
Understanding user entitlements that are out of scope for a particular role or that violate a policy	17%	16%
Requests for access are always checked against security policies before the access is approved and assigned	11%	Not rated

Q19a. How confident are you that your organization has enterprise-wide visibility for user access and can determine if it is compliant with policies?	1 & 2 combined	Q22a last year
Very confident	15%	14%
Confident	17%	16%
Somewhat confident	23%	20%
Not confident	34%	31%
Unsure	11%	19%
Total	100%	100%

Q19b. If "not confident," please select one reason.	Pct%	Q22b last year
We can't create a unified view of user access across the enterprise	25%	34%
We only have visibility into user account information but not entitlement information	21%	Not rated
We can't apply controls that need to span across information resources	12%	Not rated
We can't keep up with the changes occurring to our organization's information resources (on-boarding, off- boarding and outsourcing for management)	42%	Not rated
Total	100%	

Q20. What are the critical success factors for implementing **access governance across** the enterprise? Please rate the following 10 success factors using the following scale: 1 = Very important, 2 = important, 3 = sometimes important, 4 = not important, 5 = irrelevant	1 & 2 combined	Q23 last year
Senior level executive support	80%	78%
Ample budget	81%	77%
Identity and access management technologies	74%	70%
Well understood access policies and procedures	64%	52%
Accountability for governing user access owned by the business	85%	Not rated
Access rights assigned based on job function and responsibilities	65%	65%
Compliance controls consistently applied across the enterprise	73%	71%
Ability to automatically remediate access policy violations	56%	Not rated
Monitoring access inactivity to determine if access should be revoked	59%	Not rated
Audits by an independent third-party	24%	25%

IV. Perceived problems & remedies	
Q21. What are the key problems you face in delivering access to end-users within your organization? Please select only your top three choices.	Total%
Takes too long to deliver access to users (not meeting our SLAs with the business)	21%
Too expensive	37%
Too much staff required	14%
Can't apply access policy controls at point of change request	38%
Delivery of access to users is staggered (not delivered at the same time)	22%
Cannot keep pace with the number of access change requests that come in on a regular basis	52%
Lack of a consistent approval process for access and a way to handle exceptions	37%
Difficult to audit and validate access changes	19%
Burdensome process for business users requesting access	48%
No common language exists for how access is requested that will work for both IT and the business	10%
Other	3%
Total	300%

Q22. What are the key problems you face enforcing access compliance policies? (Please check all that apply)	Total%
Manual approach used (which is complex and cumbersome)	36%
Expensive because there are too many people required to enforce access policies	81%
Not enough IT staff	65%
No staff expertise to design and implement access controls	25%
Total	207%

Q23. What do you think are the root causes of key problems you selected above? Please assign an approximate percentage for each reason listed below.	Points
With so many information resources, it is difficult to keep pace with all the entitlement changes	4%
Business units often do not know what access to request	6%
IT operations finds it difficult to map access privileges to roles	21%
Manual access processes make it easy to circumvent procedures or policies	8%
We can't automate our access control policies across all information resources	5%
There is no accountability for who makes access rights decisions	19%
We do not have the resources to monitor and enforce compliance with access policy	13%
We do not have sufficient budget	19%
We do not have the skilled staff	5%
Total	100%

Attributions. In your opinion, how will each of the following situations affect your organization's access governance process?	Very significant	Significant
Q24a. Increasing number of regulations or industry mandates	26%	32%
Q24b. Adoption of cloud-based applications enables the business or end-users to circumvent existing access policies	39%	34%
Q24c. Outsourcing of applications and data for management	29%	23%
Q24d. The constant turnover (ebb and flow) of temporary employees, contractors, consultants and partners	35%	24%
Q24f. Availability of automated access governance technologies	38%	30%
Q24g. Constant changes to the organization as a result of mergers and acquisitions, divestitures, reorganizations and downsizing	29%	23%

V. Your role		
D1. What organizational level best describes your current position?	Pct%	Last year
Senior Executive	0%	1%
Vice President	3%	2%
Director	19%	17%
Manager	27%	40%
Supervisor	21%	Not rated
Technician	17%	Not rated
Staff	9%	38%
Contractor	2%	Not rated
Other	2%	2%
Total	100%	100%

D2. Is this a full time position?	Pct%
Yes	98%
No	2%
Total	100%

D3. Check the **Primary Person** you or your IT security leader reports to within the organization.	Pct%
CEO/Executive Committee	0%
Chief Financial Officer	3%
General Counsel	0%
Chief Information Officer	56%
Compliance Officer	5%
Human Resources VP	5%
Chief Security Officer	4%
Chief Information Security Officer	19%
Chief Risk Officer	6%
Other	2%
Total	100%

D4 Experience	Mean	Median
Total years of job experience	10.30	9.50
Total years in IT or security field	9.54	9.00
Total years on the job	4.57	5.00

D5. Gender	Pct%
Female	35%
Male	65%
Total	100%

D6. What industry best describes your organization's industry focus?	Pct%
Automotive	1%
Brokerage & Investments	2%
Communications	4%
Credit Cards	3%
Defense	5%
Education	4%
Energy	3%
Entertainment and Media	2%
Federal Government	12%
Food Service	1%
Healthcare	9%
Hospitality	2%
Manufacturing	6%
Insurance	2%
Internet & ISPs	1%
State or Local Government	3%
Pharmaceuticals	5%
Professional Services	4%
Retailing	8%
Retail Banking	11%
Services	3%
Technology & Software	5%
Transportation	2%
Total	100%

D7. Where are your employees located? (check all that apply):	Pct%
United States	100%
Canada	63%
Europe	65%
Middle east	12%
Asia-Pacific	40%
Latin America	39%

D8. What is the worldwide headcount of your organization?	Pct%
Less than 500	7%
500 to 1,000	9%
1,001 to 5,000	25%
5,001 to 25,000	30%
25,001 to 75,000	17%
75,001 to 100,000	6%
101,000 to 150,000	3%
150,000+	3%

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.