

Sponsored by



Independently Conducted by



Presents

2008 National Survey on Access Governance

US Study of IT Practitioners

Published by Ponemon Institute LLC

January 31, 2008

2008 National Survey on Access Governance

Prepared by Dr. Larry Ponemon, January 31, 2008

I. Why is this study important?

When employees, temporary employees, contractors and partners have inappropriate access to information resources, companies are subject to serious compliance and business risks. To mitigate this risk, companies need to have in place a governance framework that will ensure access to corporate information resources is appropriate and to avoid any misuse that could negatively impact an organization.

According to recent Ponemon Institute research, insider threats represent one of the most significant information security risks for organizations around the globe. Failing to properly control access for employees, temporary employees, contractors and partners is one reason why insiders inadvertently cause information destruction, leakage or theft.

Aveksa and Ponemon Institute are pleased to present the results of the 2008 National Survey on Access Governance. In this study, we surveyed almost 700 experienced IT practitioners from U.S. business and governmental organizations. According to participants in our study, user access governance is important in order to reduce the cost and burden associated with achieving compliance, to improve compliance with regulations and, as described above, to reduce the risk of insider negligence and malicious insiders.

The overall objective of this study is to learn from the perspective of IT security & compliance practitioners how well access governance is being achieved within their organizations. Following are some of the questions we sought answers to:

- 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 he or she is accessing?
- What are the critical success factors in an access governance program?

Respondents have a median of almost 10 years business experience and almost nine years IT/information security experience. They have approximately four years experience in their current position. Seventeen percent are at the director level and 40% are at the manager level. More than half (55%) are employed by companies that are publicly-traded on one or more major stock exchanges in the United States.

II. Executive summary

Access governance ensures that users of information resources, which include applications, files and data, have appropriate rights to specific information resources that are needed to do their job and are appropriate for their role within the organization. In other words, access rights should be no more and no less than necessary to fulfill a particular job function or business role.

Another purpose of access governance is to ensure that an end user's right to use or view business information resources does not violate compliance regulations as required by financial controls legislation (Sarbanes-Oxley, J-SOX, Euro-SOX, Bill 198), various data protection and privacy regulations (GLBA, PCI, HIPAA, PIPEDA, CA1386, EU Data Protection Directive) and industry mandates (Basel II, Solvency II, NASD, FERC/NERC)..

The findings from our study illustrate the challenges organizations face in having an effective governance process. Based on responses to our survey, we have identified four major challenges to implementing an effective access governance framework:

- Organizations are finding it difficult to enforce access policies in a consistent fashion across the entire enterprise.
- Collaboration among business units and security, audit and compliance teams to ensure accountability for governing access and to understand roles and responsibilities is viewed as critical but is not being achieved.
- Organizations are not able to keep pace with changes to users' roles as a result of transfers, terminations and revisions to job responsibilities. As a result, they face serious noncompliance and business risks.
- Senior management does not seem understand the risk of inappropriate user access and what resources are needed to prevent compliance and business risks.

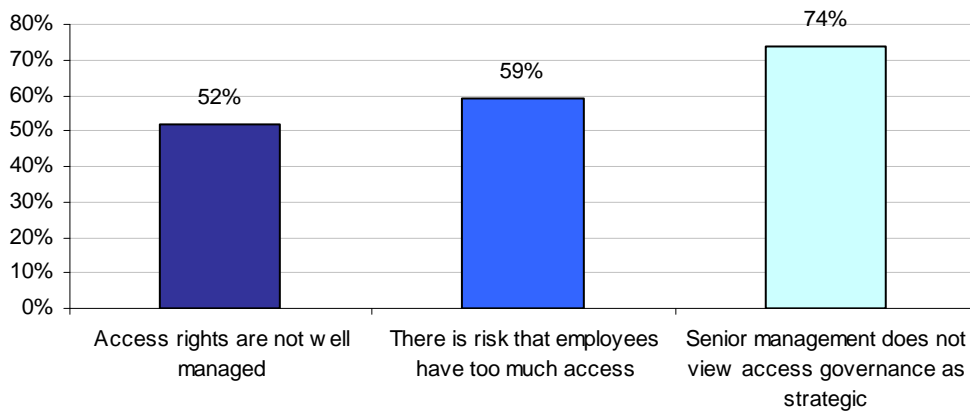
Following are the most salient findings of this survey. Please note that all survey results are included in tabular format at the conclusion of this report.

1. The current process of assigning access rights creates serious compliance and business risks.

Bar Chart 1 shows that 52% strongly disagree, disagree or are unsure that the process of assigning access rights is *well-managed and tightly controlled* within their organizations. Fifty-nine percent of respondents strongly disagree, disagree or are unsure that there is little risk that employees, temporary employees and contractors have *too much access* to information resources. Seventy-four percent believe that senior management does not view, or is unsure that, access governance is a strategic security imperative.

The pattern of responses to four questions (see Questions 1 to 4 in the accompanying appendix) suggests that many respondents see their organizations as ineffective in managing access rights to critical information resources.

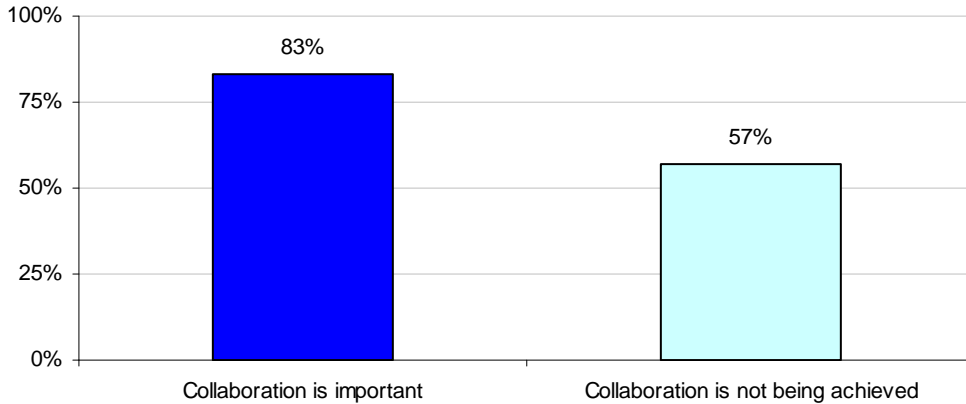
Bar Chart 1
Attributions about access governance



2. Collaboration is believed to be key to a successful access governance program, but it is not achieved.

Bar Chart 2 shows that 83% of respondents believe collaboration among business units, audit and compliance, and IT security functions is either very important or important to achieving compliance with regulations and mandates. This suggests that respondents believe that the domain knowledge that these key stakeholders have regarding business roles and responsibilities will help ensure that no regulatory compliance violations will occur when granting access.

Bar Chart 2
How important is collaboration and is it being achieved?

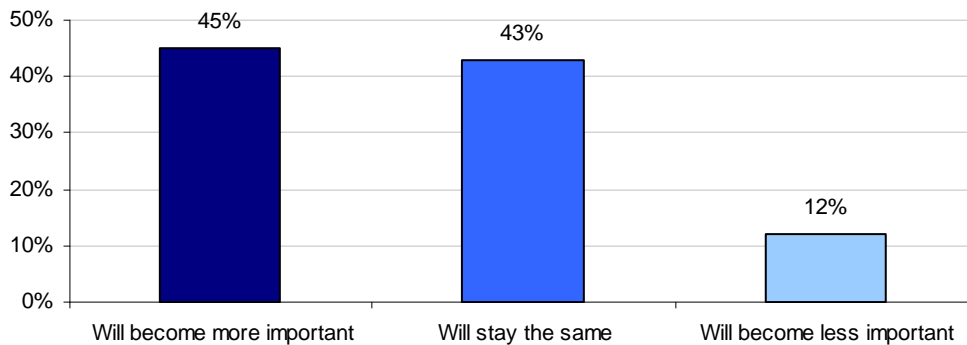


Despite the importance of collaboration, 57% report that business units, audit/compliance and IT security teams do not collaborate (or are unsure about collaboration) to achieve effective access compliance within their organizations.

3. While access governance does not have support from senior leadership, respondents believe it will continue to be important.

As shown in Bar Chart 1 above, respondents don't believe senior leadership views access governance as *strategic* to achieving IT or information security goals. However, Bar Chart 3 reports 45% of all respondents believe access governance will become *more important* to their organizations over the next two years. Another 43% believe importance will stay the same, and only 12% believe access governance will become less important to their organizations.

Bar Chart 3
Will access governance become more important over time?



Fifty-one percent of respondents who report access governance will become more important to their organizations believe that reducing access-related risks that can negatively impact the business is critical. Thirty-seven percent believe that there will be more regulations to comply with and 35% believe that access governance will become more important due to the constant change in user roles within the organization and the impact that would have on compliance with regulations.

Eighty-five percent of those who believe access governance will become less important have confidence that access-related risks will be reduced as a result of improvements in access rights management technologies. Thirty-six percent believe there will be a decrease in risk of noncompliance with regulations. Only 18% of this group believes that there will be fewer regulations to comply with.

This finding suggests that because access is a core part of most compliance mandates, the IT security organization's ability to streamline access authorization and certification through access rights management technologies will reduce noncompliance risks.

4. Access risk is only being classified at the information resource level and is not mapped to a user's functional responsibilities.

Bar Chart 4 shows 73% of respondents report that their organizations determine risk to information based on the inherent risk of different data types rather than based on users' role or function (33%). This result suggests that organizations might find it too difficult to manage access rights at the individual level because of changing business roles and responsibilities with respect to information resources.

In fact, according to responses in Question 21, only 27% of respondents believe that their ability to assign access rights based on job function is excellent or good, while 55% of respondents to the same question described their ability as either poor or nonexistent, including 42% who reported that it is not performed at all at their organizations. Further, only 16% believe they do an excellent or good job at understanding when entitlements are out of scope for a particular job function.

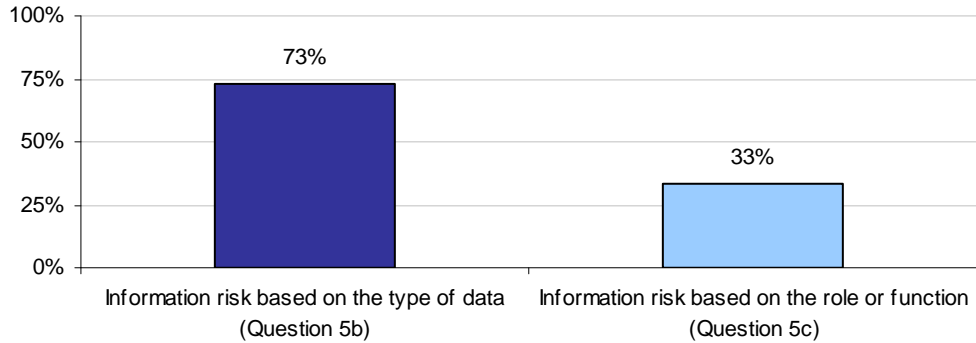
These findings suggest a huge risk for organizations because of having large numbers of individuals accessing information resources that are not in alignment with their job function. In addition, access governance needs to take into consideration more than just the type of data users handle.

Without understanding a user's job function and the type of entitlements/permissions he or she has within a given resource, it is difficult to properly manage risk associated with segregation of duties and privileged user accounts. Accordingly, 66% of respondents report they do a fair or poor job of monitoring segregation of duties.

Bar Chart 4

How do you classify information risk?

Subsample of 63% of all respondents who said that their organization's information resources are classified by risk. The two bars are from separate survey items and, hence, do not sum to 100%.



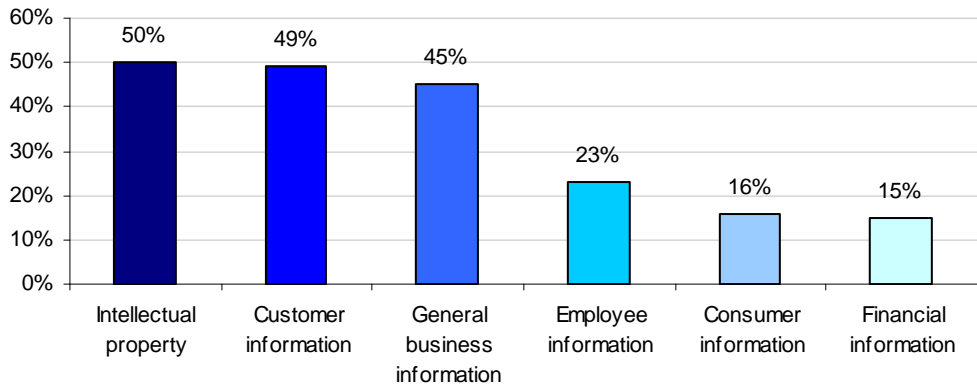
5. Intellectual property is considered most at risk.

In Bar Chart 5, intellectual property (50%), customer information (49%) and general business information (45%) are considered most at risk because of poor access governance within their organizations. Least at risk are financial information (15%), consumer information (16%), and employee records (23%). The fact that financial information is considered the least risky information type may be due to the fact that organizations have put a governance framework of controls in place to meet compliance requirements mandated by the Sarbanes-Oxley Act.

Bar Chart 5

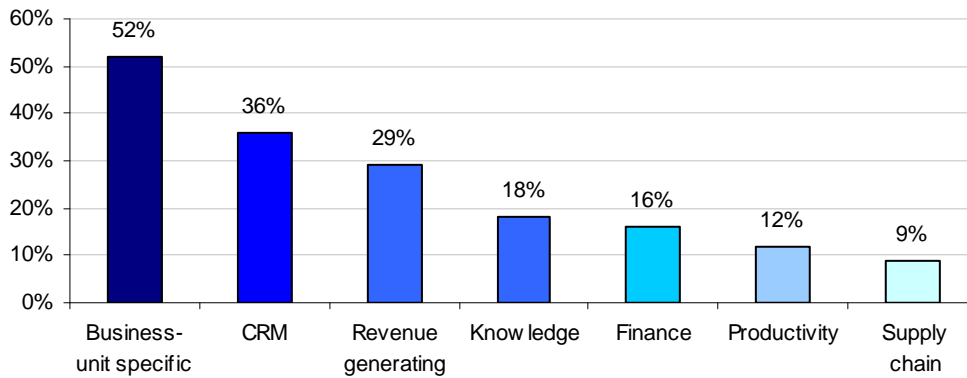
Information most at risk because of ineffective access governance

Chart does not sum to 100% because more than one response was allowed



According to Bar Chart 6, applications most at risk according to respondents include business-unit specific (52%), CRM (36%) and revenue generating (29%) applications, respectively. This finding supports the above result that customer information is extremely vulnerable because of poor access governance. CRM and revenue generating applications will typically contain significant amounts of customer information – such as for call center operations or sales force automation applications.

Bar Chart 6
Applications most at risk because of ineffective access governance
 Does not sum to 100% because more than one response was allowed

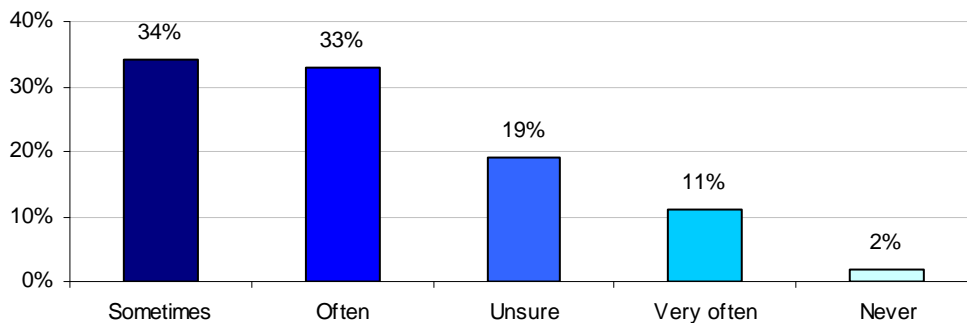


Financial applications are viewed as less at risk and this can possibly be attributed to the deadlines faced by organizations in complying with financial control legislation such as SOX. The same degree of controls should be extended to include users' access to all information resources.

6. Risk to organizations' information resources has moved inside.

According to Bar Chart 7, organizations are increasingly at risk because of individuals having too much access to information resources that are not pertinent to their job description, function or role. This situation could be created by the challenge of keeping pace with the amount of change to roles and user access within an organization.

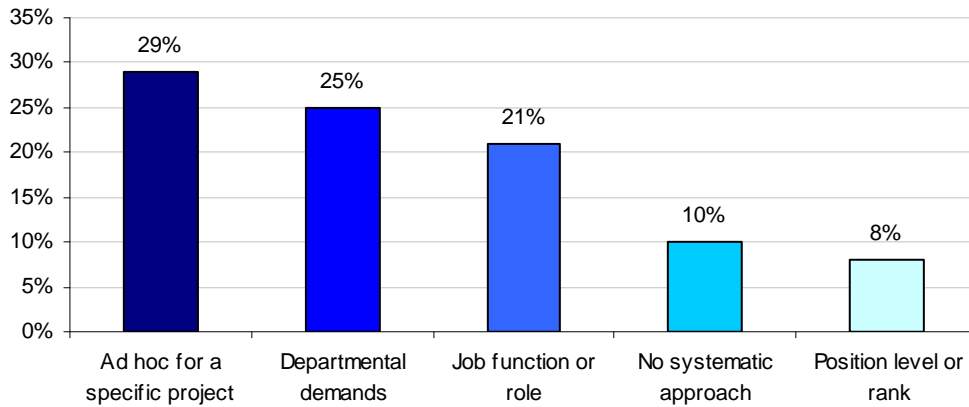
Bar Chart 7
Do employees have too much access to information resources not pertinent with their job function?



7. The process of granting access tends to be ad hoc rather than based upon well-defined business policies that are centrally controlled and consistently applied.

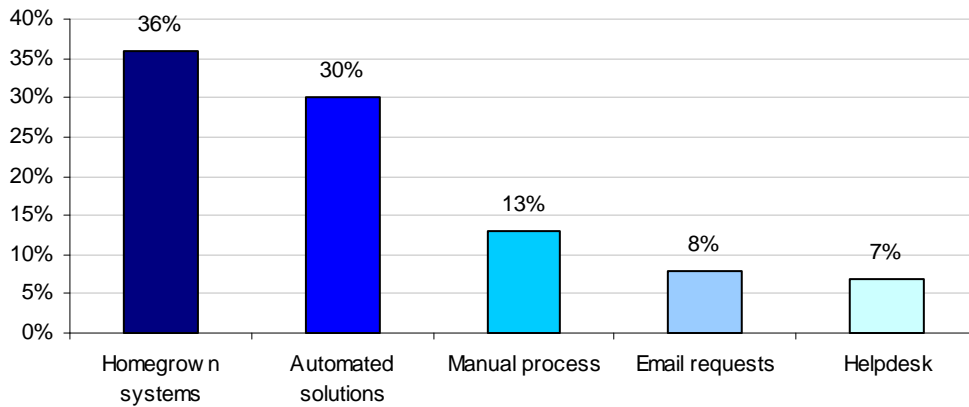
Bar Charts 8 and 9 describe the process for assigning access rights in respondents' organizations. As shown in Bar Chart 8, access rights are assigned on an ad hoc basis for specific projects (29%), in response to demands of specific departments (25%), or to support job function and role (21%). Only 8% of respondents' organizations assign access rights based on solely on the employee's position level or rank. Another 10% state there is no systematic approach or process for granting access rights.

Bar Chart 8
How is access to information assets granted?



According to Bar Chart 9, when asked what process organizations use for responding to requests for access to information resources, the highest percentage (36%) indicate that homegrown access control systems are used followed by off-the-shelf automated solutions (30%) and manual processes (13%). The process used to certify user access is most often a manual process (32%) followed by an automated off-the-shelf system (23%).

Bar Chart 9
What process is used for granting user access?



Taken together, our findings indicate that the distributed nature of the organization has resulted in a breakdown in centralized policy management. Application owners are distributed throughout the organizations which can contribute to the problem of ensuring proper access. The ad-hoc approach can contribute to excessive user access. If access is granted based on a time period or project, is there a process in place for ensuring that entitlements that were granted are now revoked when no longer needed. If there is no regular review of access, there is no way to mitigate the risk.

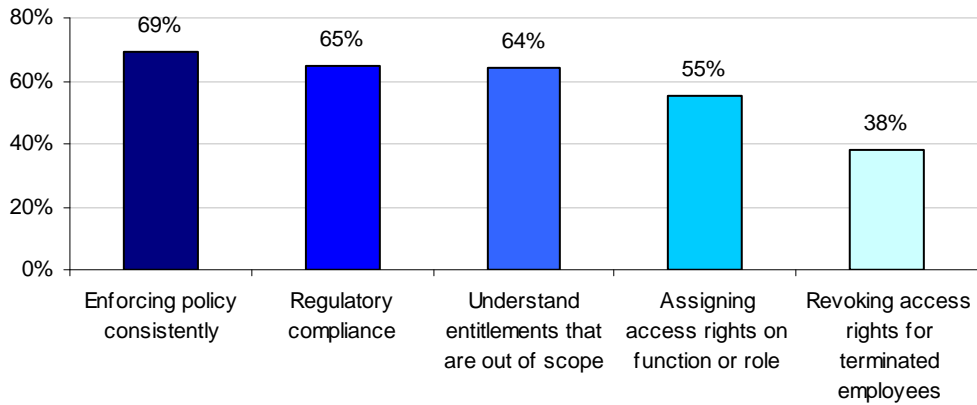
8. User access policies are not enforced.

Bar Chart 10 shows the access governance tasks that are poorly performed. These findings indicate that organizations have a serious problem in making sure that users do not have access to information resources that could put it at risk.

Bar Chart 10

Does your organization enforce user access policies?

The percent of respondents who said that a task is done poorly or is not done.

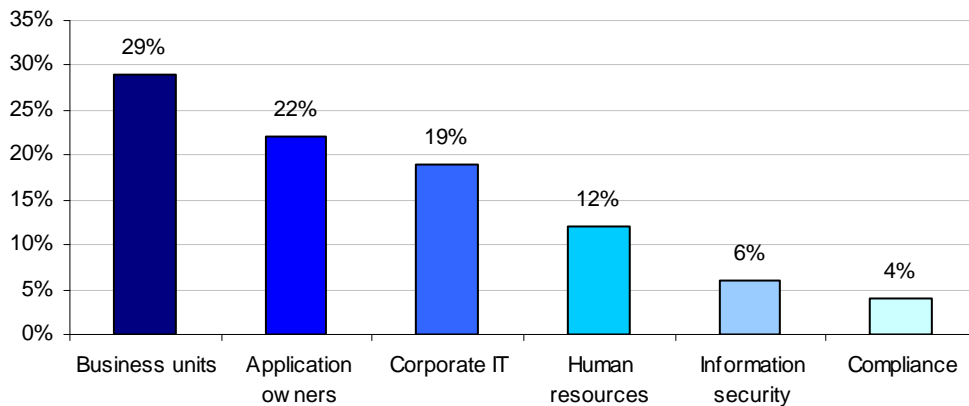


9. Accountability for granting access is hard to pinpoint.

Who is most accountable for managing access governance? Although there is no clear majority believed to be accountable, Bar Chart 11 shows that business unit leaders are perceived as *most responsible* for governing access rights (29%), followed by application owners (22%) and corporate IT (19%).

Bar Chart 11

Who is most accountable for access governance?

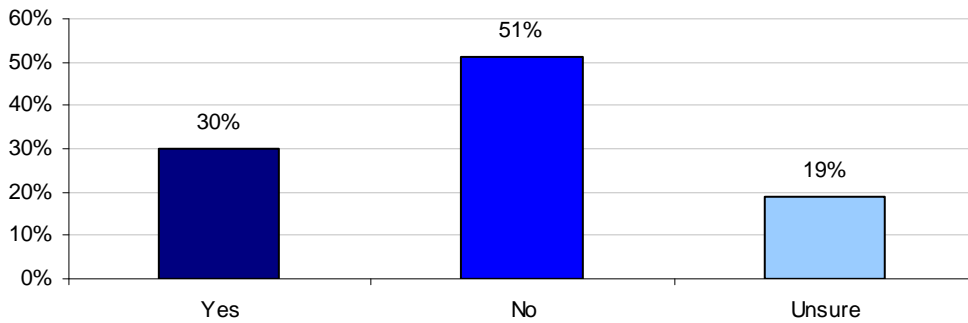


Consistent with the above finding, 55% of respondents believe business units are by far the most responsible for conducting role reviews and certification. This finding suggests that responsibility and accountability must be based on collaboration throughout the organization.

9. Access is creating potential risks because access is not sufficiently reviewed and checked.

As shown in Bar Chart 12, only 30% of respondents state that their organizations make sure user access policies are validated and checked. Organizations are at risk because user job functions and responsibilities are not static but dynamic. Therefore, regular reviews and monitoring of change is necessary to ensure that compliance objectives and business risk tolerances are met.

Bar Chart 12
Is the enforcement of user access policies validated or checked?

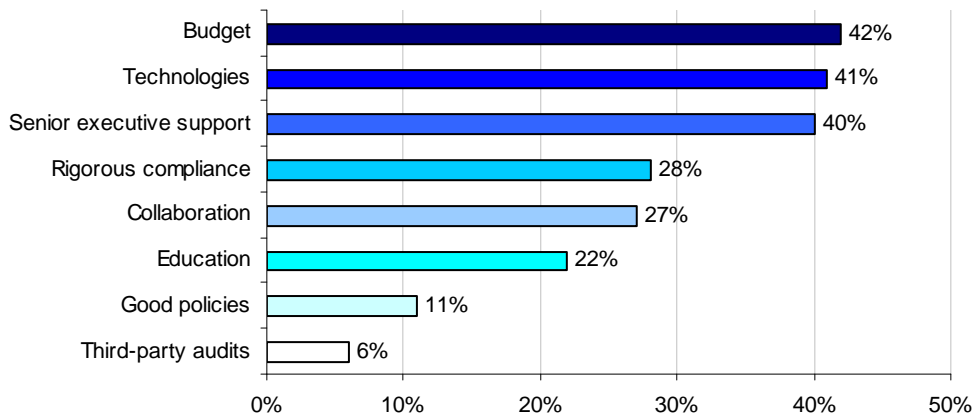


In addition to data in the above bar chart, 54% of respondents' organizations use some form of business-centric roles to determine the appropriateness of user entitlements (see Question 14a). However, less than half (49%) state their organizations regularly review or certify the appropriateness of these business-centric roles (see Question 14b).

10. What are the critical success factors to access governance?

As shown in Bar Char 13, ample budget (42%), implementing enabling technologies (41%), obtaining senior executive support (40%) and strict enforcement of non-compliance (28%) are the top four critical success factors according to respondents.

Bar Chart 13
What are the critical success factors to achieving access governance?



According to respondents, the least important factors are: audits by third parties (6%), good policies (11%) and employee education (22%). This finding suggests that IT practitioners believe technologies are essential and the purchase of such technologies requires financial resources and senior executive buy-in.

III: Caveats

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 information technology 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.

IV: Sample

A random sampling frame of 11,890 adult-aged individuals who reside within the United States was used to recruit participants to this web survey. Our randomly selected sampling frame was selected from three national mailing lists of IT and IT security professionals. In total, 813 respondents completed their survey results during within a 10-day research period. Of returned instruments, 118 survey forms were rejected because of reliability checks. A total of 695 surveys were used as our final sample. This sample represents a 5.8% net response rate. The margin of error on all adjective scale and Yes/No/Unsure responses is $\leq 3\%$.

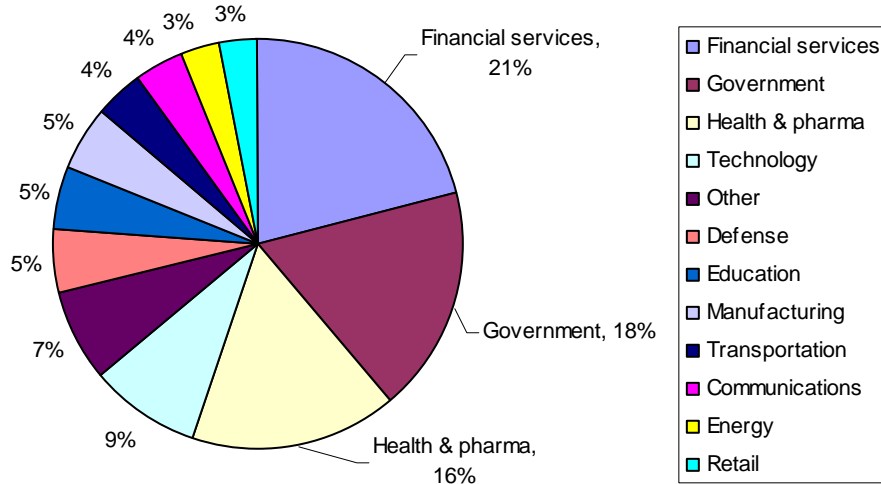
Over 85 % of respondents completed all survey items within 10 minutes. Following are key demographics and organizational characteristics for U.S. respondents. Table 1a reports the most frequently cited job functions/titles of respondents (top five). Table 1b provides the self-reported organizational level of respondents. As can be seen, the majority of respondents are at the manager (40 %) or staff/technician (38 %) levels, respectively.

Table 1a: Job functions (based on top 5 titles only)	Pct%
IT security	12%
IT operations	10%
Network security	9%
Audit, compliance or QA	9%
Information management	8%
Other	52%
Total	100%

Table 1b: Organizational levels	Pct %
Senior executive	1%
Vice president	2%
Director	17%
Manager	40%
Staff/Technician	38%
Other	2%
Total	100%

On average, respondents have almost ten years of experience in the information management or security fields, and over three years of experience in their current position. In total, 63% of respondents were males and 37% females. While results are skewed on the gender variable (more male than female respondents), this result is consistent with known demographics about the corporate IT fields in North America.

Pie Chart 1: Industry Distribution



Pie Chart 1 reports the %age distribution of respondents by their organization’s primary industry classification. As shown, over 21% of respondents are employed by financial service companies (including insurance, banking, credit cards, brokerage and investment management), and 18% work for federal or local government. Another 16% work in the health care and pharmaceutical sector.

Table 2a reports the organization’s economic structure, showing that the majority of respondents’ companies work for organizations that are publicly traded on a major exchange. Table 2b provides the approximate headcounts of these organizations. As can be seen, 39% of respondents are employed by larger-sized organizations (with more than 25,000 employees).

Table 2a. Economic structure	Pct%
Major exchange (NYSE, NASDAQ)	55%
Minor exchange	5%
Not publicly traded	40%
Total	100%

Table 2b. Corporate headcount	Pct%.
Less than 500 people	3%
500 to 1,000 people	3%
1,001 to 5,000 people	15%
5,001 to 25,000 people	40%
25,001 to 75,000 people	27%
More than 75,000 people	12%
Total	100%

V: Implications & Recommendations

Organizations need to consider the benefits of having an enterprise-wide access governance process that is based on collaboration among different business functions. The objective is to have a more effective process for managing access rights, ensuring that policies are enforced consistently and understanding the business function that is accountable. Here are some specific recommendations that directly relate to the findings of our survey:

- 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, organizations need to ensure that they do not hinder the ability of individuals to have access to information resources critical to their productivity. To do this, you must understand what sensitive and confidential information resources based

on their roles within the organization individuals need to access in order to support business goals and objectives. Further, you will need to manage changes to a user's role to ensure that he or she continues to have the correct access rights for a given job function.

- Create well-defined business policies for the assignment of access rights. These policies should be centrally controlled to ensure that they are enforced in a consistent fashion across the entire enterprise.
- Understand how to make the case for building an enterprise-wide access governance process to senior management. Factors to include are the fines and penalties for noncompliance and downtime as a result of negligence that causes operational problems. With respect to data breaches, it is the cost of notification, customer attrition and loss of reputation that can severely impact an organization's bottom line. This will help ensure there is an ample budget and collaboration among business units to enforce user access policies.
- Track and measure the organization's ability to enforce user access policies. This includes how effective the process is in managing 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 your organization to have visibility to all user access across all information resources and entitlements to these resources. Technologies that automate access authorization, review and certification will limit the risk of human error and negligence.

In summary, the importance of this study is to better understand current access governance practices and where organizations may be at greatest risk because of systemic governance gaps. Our findings show that IT practitioners generally see the need for a strategic, unified approach to access governance and related responsible information management practices.

Despite these perceptions, our findings also suggest that many organizations are facing significant information risks because of ad hoc or inconsistent approaches to access management activities across the enterprise. The next section is an Appendix showing the %age frequencies of all survey questions included in our survey instrument.

Appendix 1: Detailed Survey Results

Sample characteristics	Totals
Total sample frame	11890
Total bounce backs	1320
Total response	813
Rejected surveys	118
Final sample	695
Response rate	5.8%

Attributions: Please rate your opinion for Q1 to Q4 using the scale provided below each statement.

Q1. {Attribute 1} In my organization, the process for assigning access rights to Information resources is well managed and tightly controlled.	Pct%
Strongly agree	24%
Agree	24%
Unsure	29%
Disagree	15%
Strongly disagree	9%
Total	100%

Q2. {Attribute 2} In my organization, there is little risk that employees, temporary employees or contractors would have too much access to information assets.	Pct%
Strongly agree	17%
Agree	24%
Unsure	28%
Disagree	19%
Strongly disagree	12%
Total	100%

Q3. {Attribute 3} In my organization, senior leadership views governing access as a strategic objective for information security.	Pct%
Strongly agree	9%
Agree	17%
Unsure	20%
Disagree	32%
Strongly disagree	22%
Total	100%

Q4. {Attribute 4} In my organization, the implementation of effective access control requires good collaboration across different functional areas including IT security, business units and compliance/audit teams.	Pct%
Strongly agree	29%
Agree	36%
Unsure	9%
Disagree	12%
Strongly disagree	14%
Total	100%

Q5a. Does your organization make decisions regarding granting access on risk factors?	Pct%
Yes	63%
No	17%
Unsure	20%
Total	100%

Q5b. If yes, do you classify information resources based on risk?	Pct%
Yes	73%
No	21%
Unsure	6%
Total	100%

Q5c. If yes, do you classify roles based on risk?	Pct%
Yes	33%
No	57%
Unsure	10%
Total	100%

Q6. What types of data do you consider to be most at risk in your organization? Top two choices.	Total%
Customer information	49%
Consumer information	16%
Employee information	23%
Financial information	15%
General business information	45%
Intellectual property	50%
Total	198%

Q7. What type of applications do you consider to be most at risk in your organization? Top two choices.	Total%
Finance/ERP applications	16%
CRM applications	36%
Supply chain management applications	9%
Revenue generating applications	29%
Business unit specific applications	52%
Productivity applications	12%
Knowledge applications	18%
Total	172%

Q8. What best describes the process for assigning access rights in your organization today? Please select one <u>best</u> choice.	Pct%
An "ad hoc" process	31%
Determined by well-defined policies that are <u>centrally</u> controlled by corporate IT	25%
Determined by well-defined policies that are <u>not centrally</u> controlled by corporate IT	3%
Determined by well-defined policies that are <u>centrally</u> controlled by business or application owners	8%
Determined by well defined policies that are <u>not centrally</u> controlled by business or application owners	30%
Unsure	11%
Total	100%

Q9. How often does an employee, temporary employee or independent contractor have too much access to information assets that are not pertinent to their job description?	Pct%
Never	2%
Sometimes	34%
Often	33%
Very often	11%
Unsure	19%
Total	100%

Q10. How is access to information assets granted to employees, temporary employees or independent contractors within your organization?	Pct%
On a need to know basis based on a project or ad hoc basis	29%
On a need to know basis based on function or job role	21%
On the employee's position level or rank	8%
On the employee's department and title	25%
No systematic approach or process for granting access rights exist	10%
Combination of job function and job title	16%
Total	100%

Q11. Who has accountability for granting user access to information resources?	Pct%
Information technology department	19%
Information security department	6%
Compliance department	4%
Business unit managers	29%
Application owners	22%
Human resource department	12%
Unsure	8%
Total	100%

Q12. What process is used for granting user access to information resources?	Pct%
Manual process	13%
E-mail requests	8%
Homegrown access control systems	36%
Automated solutions (off the shelf system)	30%
Help desk system (tickets)	7%
Unsure	6%
Total	100%

Q13. What process is used to certify user access?	Pct%
Manual process	32%
Email	10%
Homegrown system	21%
Automated system (off the shelf system)	23%
Other	8%
Unsure	6%
Total	100%

Q14a. Does your organization use business-centric roles to make determinations on what user entitlements are appropriate?	Pct%
Yes	54%
No	46%
Total	100%

Q14b. If yes, are roles regularly reviewed and certified for appropriateness?	Pct%
Yes	49%
No	51%
Total	100%

Q14c. If yes (both 14a & 14b) Who is responsible for conducting role reviews and certification?	Pct%
IT security teams	16%
Business units	55%
Audit/compliance teams	29%
Other	1%
Total	100%

Q17. Is the enforcement of user access policies validated or checked?	Pct%
Yes	30%
No	51%
Unsure	19%
Total	100%

Q18. Which department or functional area is <u>most accountable</u> for ensuring that access control policies or procedures are enforced?	Pct%
Information technology department	9%
Information security department	10%
Compliance department	11%
Business unit managers	31%
Application owners	20%
Human resource department	19%
Other (please specify)	0%
Unsure	1%
Total	100%

Q19a. Is there collaboration among business units, audit/compliance and IT security teams to achieve effective access compliance with your organization?	Pct%
Yes	44%
No	50%
Unsure	7%
Total	100%

Q19b. If yes, how important is collaboration among these three functions to achieving effective access compliance?	Pct%
Very important	45%
Important	38%
Sometimes important	15%
Not important	2%
Irrelevant	0%
Total	100%

Q20. How does your organization control privileged users' access to information resources and/or systems?	Pct%
Technology-based identity and access controls	25%
Manually-based identity and access controls	20%
A combination of technology and manually-based identity and access controls	44%
Access to sensitive or confidential information is not really controlled	7%
Unsure	5%
Total	100%

Q21. How well is your organization able to enforce user access policies for the following tasks? Please use the following scale to rate each task provided. Scale: 1 = excellent, 2 = good, 3 = fair, 4 = poor, 9 = task is not performed.	1	2	3	4	9	Total%
Assigning access rights based on job function or role	20%	7%	18%	13%	42%	100%
Managing changes to a user's role (i.e. when a contractor becomes a full-time employee or when an employee is transferred to another department)	17%	15%	37%	29%	2%	100%
Revoking access rights upon an employee's termination	13%	10%	38%	38%	0%	100%
Enforcing access policies in a consistent fashion across all enterprise information resources	2%	15%	14%	11%	58%	100%
Monitoring and managing access rights of privileged user accounts (such as database administrators or system administrators)	17%	18%	49%	14%	1%	100%
Monitoring segregation of duties	5%	29%	30%	36%	1%	100%
Keeping detailed logs showing all privileged users' access (authorized or unauthorized)	11%	16%	39%	34%	1%	100%
Meeting regulatory compliance objectives and providing evidence of compliance	3%	11%	21%	29%	36%	100%
The ability to understand user business roles and appropriate entitlements	11%	6%	31%	24%	27%	100%
The ability to understand user entitlements that are out of scope for a particular role	9%	7%	19%	38%	27%	100%
Educating end-users about access control policies and procedures	4%	10%	18%	19%	49%	100%
Implementing identity audit and roles management technologies	18%	10%	8%	12%	52%	100%

Q22a. How confident are you that your organization has visibility to all user access across all information resources and entitlements to these resources?	Pct%
Very confident	14%
Confident	16%
Somewhat confident	20%
Not confident	31%
Unsure	19%
Total	100%

Q22b. If "not confident," please select <u>one</u> reason.	Pct%
We can't create a unified view of user access across the enterprise	34%
We can't extract user access data from all applications	32%
We can only access user account information from applications but not entitlement information	34%
Total	100%

Q23. What are the critical success factors for implementing access governance across the enterprise? Please rate the following 11 success factors using the following scale: 1 = Very important, 2 = important, 3 = sometimes important, 4 = not important, 5 = irrelevant.	1	2	3	4	5	Total%
Senior level executive support	40%	38%	11%	11%	0%	100%
Ample budget	42%	35%	21%	2%	0%	100%
Identity and access management technologies	41%	29%	19%	3%	9%	100%
Clear and concise policies and standard operating procedures	11%	41%	30%	11%	7%	100%
Collaboration across different business units including IT security, business units and audit/compliance teams	27%	32%	25%	1%	15%	100%
Employee education or training	22%	33%	33%	12%	0%	100%
Access rights assigned using role or function-based methods	24%	41%	24%	2%	9%	100%
Rigorous compliance procedures	28%	43%	17%	12%	0%	100%
Strict enforcement of non-compliance	39%	47%	10%	1%	2%	100%
Monitor privileged users	15%	33%	43%	6%	3%	100%
Audits by an independent third-party	6%	19%	33%	24%	18%	100%

Q24a. In your opinion, how will the importance of access governance in your organization change over the next two years?	Pct%
It will become more important for my organization	45%
It will stay the same in terms of importance for my organization	43%
It will become less important for my organization	12%
Total	100%

Q24b. If you believe access governance will become “more important,” why do you feel this way? Please select all that apply.	Total%
More regulations to comply with	37%
User roles will constantly change	35%
Managing user access at the application level will become more complex	14%
Compliance costs will increase	19%
Accountability for governing user access will be needed	23%
Automated access governance to reduce the cost and burden on business will be needed	18%
Access-related risks that can negatively impact the business will need to be reduced	51%
Total	317%

Q24c. If you believe access governance will become “less important,” why do you feel this way?	Total%
Fewer regulations to comply with	18%
Decrease in risk of noncompliance with regulations	36%
Improvement in IT security education	14%
New access rights management technologies will reduce access control risks and cost	85%
Decrease in the number of temporary employees and contractors	0%
Total	153%

Q25 In your opinion, why is access governance important? Please select your top three reasons.	Total%
To reduce the risk of insider negligence	49%
To reduce the risk of malicious insiders	23%
To reduce the risk of perimeter attacks	8%
To enable third parties and outsourcers access to information assets	39%
To establish accountability for access rights at the right level	46%
To improve compliance with policies, procedures and law	75%
To establish trust and confidence among customers	14%
To reduce the cost and burden associated with achieving compliance	33%
To reduce risks that can negatively impact the business	75%
Total	362%

Demographics and Organizational Characteristics

What organizational level best describes your current position?	Pct%
Senior Executive	1%
Vice President	2%
Director	17%
Manager	40%
Associate/Staff	38%
Other	2%
Total	100%

Check the Primary Function where you reside within your organization.	Pct%
IT Operations	40%
Application development	10%
Compliance	11%
Research	0%
Human resources	2%
Procurement	2%
Security	28%
Risk management	8%
Total	100%

Categories	Median
Business experience	9.91
IT/security experience	8.97
Years in current position	3.82

Is your company publicly traded?	Pct%
Yes, major stock exchange (NYSE or NASDAQ)	55%
Yes, minor stock exchange	5%
No	40%
Total	100%

What is the approximate size of your IT department in terms of full-time equivalent (FTE) headcount?	Pct%
Less than 50 people	2%
Between 50 to 100 people	3%
Between 100 to 1,000 people	23%
Between 1,000 to 10,000 people	62%
Over 10,000 people	10%
Total	100%

What is the worldwide headcount of your organization?	Pct%
Less than 500 people	3%
500 to 1,000 people	3%
1,001 to 5,000 people	15%
5,001 to 25,000 people	40%
25,001 to 75,000 people	27%
More than 75,000 people	12%
Total	100%

What industry best describes your organization's industry focus?	Pct%
Airlines	1%
Automotive	0%
Agriculture	0%
Brokerage	5%
Credit Cards	3%
Defense	5%
Education	5%
Energy	3%
Entertainment and Media	1%
Federal Government	15%
Food Services	0%
Health Care	12%
Hospitality & Leisure	2%
Manufacturing	5%
Insurance	2%
Internet & ISPs	1%
Local Government	3%
Pharmaceuticals	4%
Professional Services	5%
Research	1%
Retailing	3%
Retail Banking	11%
Telecommunications & Cable	3%
Technology & Software	9%
Transportation	2%
Wireless	1%
Other	0%
Total	100%

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote from or reuse this report), please contact us by letter, phone call or email:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686
1.800.887.3118
research@ponemon.org

Ponemon Institute LLC

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 company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.