Internet2 Privilege Management Survey
Fall 2008, Final Results

Background

In mid-2008, the Internet2 Signet working group grappled with a variety of issues surrounding the future of its efforts and of privilege management within higher education in general.   Concern had been expressed from various quarters about the degree of adoption of privilege management tools (and in particular, the Signet tool) within the community. The working group knew that adoption of the existing Signet tool had been limited, but it was unclear what might be the impediments to its adoption. Was the tool too difficult to implement or use? Did Signet lack specific features of critical importance to its primary audience? Or were the issues more endemic to the community – was higher ed simply not yet ready to address privilege management at a strategic level, or perhaps, was privilege management simply not a need identified or expressed by the majority of organizations within higher education?

To help shed light on some of these matters, staff from Duke University, in collaboration with the Internet2 Signet working group, set out to conduct a survey of the community. A set of some 48 questions was devised with input from the Signet working group, with the goal of answering three primary questions:

- How well prepared are the IT infrastructures at sites within higher education to implement privilege management tools?
- How significant is the need within higher education for privilege management tools?
- What are the primary functional and technical requirements higher education organizations have for privilege management tools?

Survey questions were divided into two main groups – a set of multiple-choice and open-response questions focusing on the first two areas (site preparedness and anticipated need), which all respondents were instructed to answer, and a set of Likert scale questions focusing on the perceived importance of specific technical features to responding sites. Realizing that the responses of, for example, central IT staff might differ dramatically from those of functional business process owners in a financial accounting department, the survey was designed in anticipation of some organizations providing multiple responses.
The survey was first proffered in September 2008 to members of the Signet development group, both in an effort to collect results from those sites (which were expected to be among the most mature in their preparation for and deployment of privilege management facilities), and in an effort to collect feedback on the

instrument itself. Soon after, the survey was offered to a wider collection of sites expressing interest in Signet or in privilege management in general. An interim report was presented at the Fall 2008 Internet2 Member Meeting in October 2008, based on results from those initial respondents. Slides from the interim report are included below, in Appendix A.

Later, in November 2008, the survey was proffered to subscribers on the Educause IdM mailing list in an effort to enhance the already-collected data with responses from sites that might not have given privilege management as thorough consideration as the original respondents. This latter round of survey responses was collected through the end of calendar 2008, and along with the initial results from the Signet working groups and other interested parties, forms the basis of this report.

The actual survey instrument (in its final form, as made available to the Educause IdM group) is included below, in Appendix B.

Key Observations

A detailed review of survey responses and results follows, but a few key observations may be worthy of specific note. From the functional and "preparedness" section of the survey:

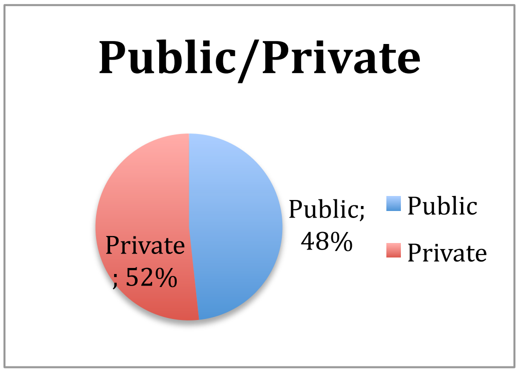
- Centralized identity management and group management were widely deployed among responding sites; centralized privilege management and policy management were less so, consistent with the hypothesis that privilege management is typically an evolutionary step into which sites may grow after deploying basic identity management and group management facilities. The survey results suggest that most sites are well prepared to take advantage of group management tools, and many are well prepared or nearly prepared to take advantage of privilege management tools.
- An overwhelming majority of sites (81%) indicated that they saw a need to develop privilege management policies; only a small fraction (6%) indicated that they already had such policies in place, supporting the hypothesis that a policy gap exists within higher ed institutions that may interfere with the widespread adoption of centralized privilege management tools.
- Responding sites dissatisfied with their current privilege management approaches outnumbered those expressing full satisfaction with their current approaches roughly two to one.
- Responding sites reporting their privilege management strategies as partially centralized (with some critical applications using central privilege management and less critical applications fending for themselves) outnumbered others by almost three to one.

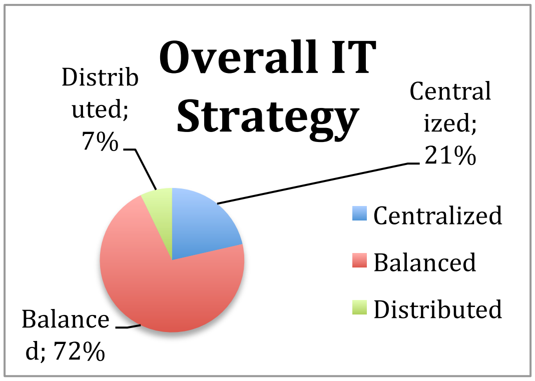
From the technical requirements section of the survey:

- The most commonly cited problems respondents expected could be addressed through enhanced privilege management were delays and inaccuracies in the onboarding and offboarding of new institutional affiliates, the so-called "privilege snowball" effect, and the lack of transparency and auditability in privileging practices and processes.
- The most sought-after features in a privilege management solution were coarse-grained privileging based on broad user affiliations, target-dependent privilege qualifications, and role- or group-based privilege management support. The least sought-after features were support for manual override of automated privileging processes, timed or triggered attestations, and temporary privilege transfer

Overall, public institutions tended to be slightly more centralized than private institutions, and tended to express more interest in auditing, reporting, and policy management features, while private institutions tended to be more distributed in their IT strategies, and focused more intently on automation, workflow, and granularity of privileging controls.

Survey Results: Overview





A total of 25 organizations provided a total of 29 responses to the survey. Both public and private institutions were well represented, with slightly more representation among private (52%) than public (48%) organizations. By far the majority of respondents characterized their institutions' overall IT strategies as either highly centralized or roughly balanced between centralized and distributed – only a small fraction (7%) indicated that their overall IT environments were mostly or completely decentralized. Centralization was slightly more common among public institutions than private institutions.

Of the 25 organizations responding to the survey, 18 organizations provided answers to all of the functional and readiness questions in the survey, while seven (six public, one private) answered only the initial "demographic" questions in the survey. Of the 18 organizations providing answers to the full set of functional and readiness questions, 16 (nine private, seven public) provided answers to the more technical, Likert-scale questions in the latter half of the survey.

Functional Questions

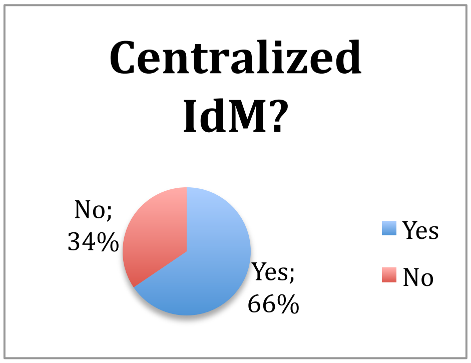
Readiness Questions

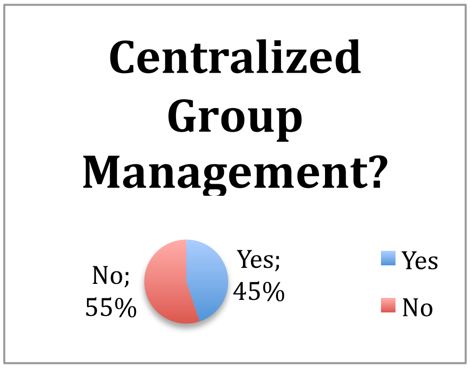
In discussions with the Signet working group, a sense developed that privilege management is something of an evolutionary outgrowth of other features of an organization's IT infrastructure, and particularly its identity management strategy. It profits an organization little to deploy tools for managing privileges across systems and application environments if the organization lacks a coherent strategy for identification and authentication, or if the organization has not already begun the process of somehow grouping individuals' electronic personae along basic lines of affiliation or responsibility. Without some basic identity management infrastructure in place, it was expected that an institution's chances of successfully deploying any privilege management tools would be limited.

To help characterize the overall state of identity management infrastructures at responding sites, the survey included four yes-no questions (and associated free-response questions) about existing identity management infrastructures:

- Does your organization currently employ centralized identity management services?
- Does your organization currently employ centralized group management tools? If so, which ones, and if not, do you plan to deploy group management within the next 12 months?
- Does your organization currently employ centralized tools for privilege management? If so, how well do your tools meet current and expected future needs, and if not, do you have plans to deploy privilege management tools within the next 12 months?
- Does your organization currently employ automated tools for managing policies or business rules pertaining to access to data or IT facilities?

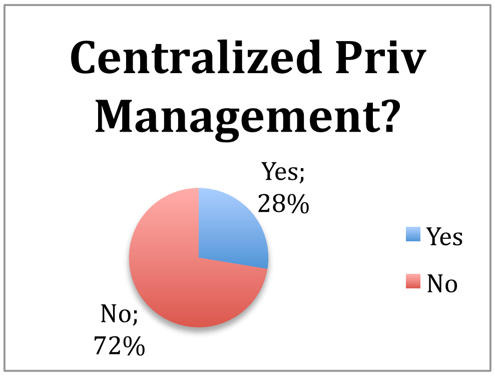
Overall responses to these questions are summarized in the charts below

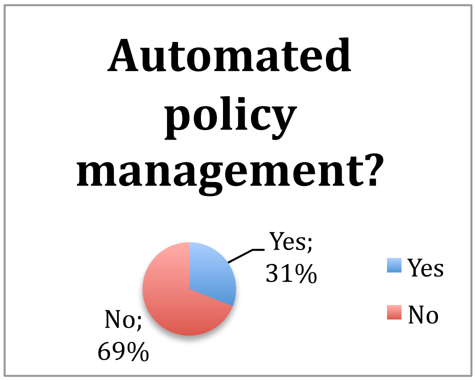




Overall, centralized identity management was comparatively ubiquitous among responding sites, with 66% of responding sites indicating that they employ some form of centralized identity management. Private institutions were over 50% more likely to be using centralized identity management than public institutions.

Centralized group management tools were similarly well deployed across responding sites, with 45% of respondents indicating that their sites had deployed some form of central group management. 42% of the sites using centralized group management tools reported they have deployed Grouper, and another 28% indicated that they are using LDAP groups directly to manage groups at their sites.



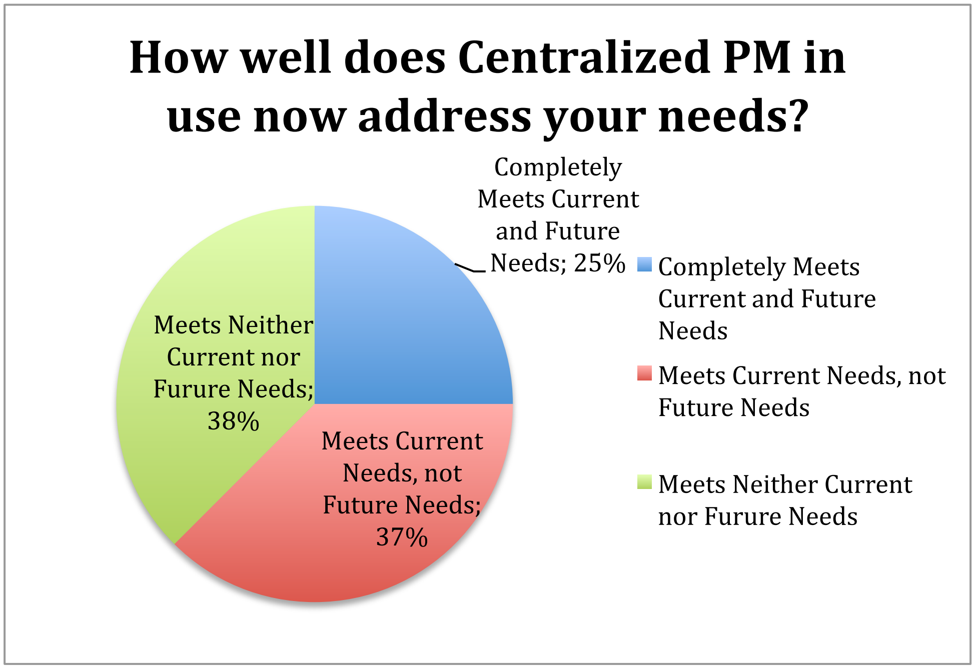


Centralized privilege management facilities appear far less widely deployed among respondents' sites. Only 28% of responding sites indicated that they had some form of centralized privilege management in use. Centralized privilege management was relatively more common among private institutions (33% of whom indicated they were using centralized privilege management) than public institutions (only 21% of whom indicated they were using centralized privilege management).

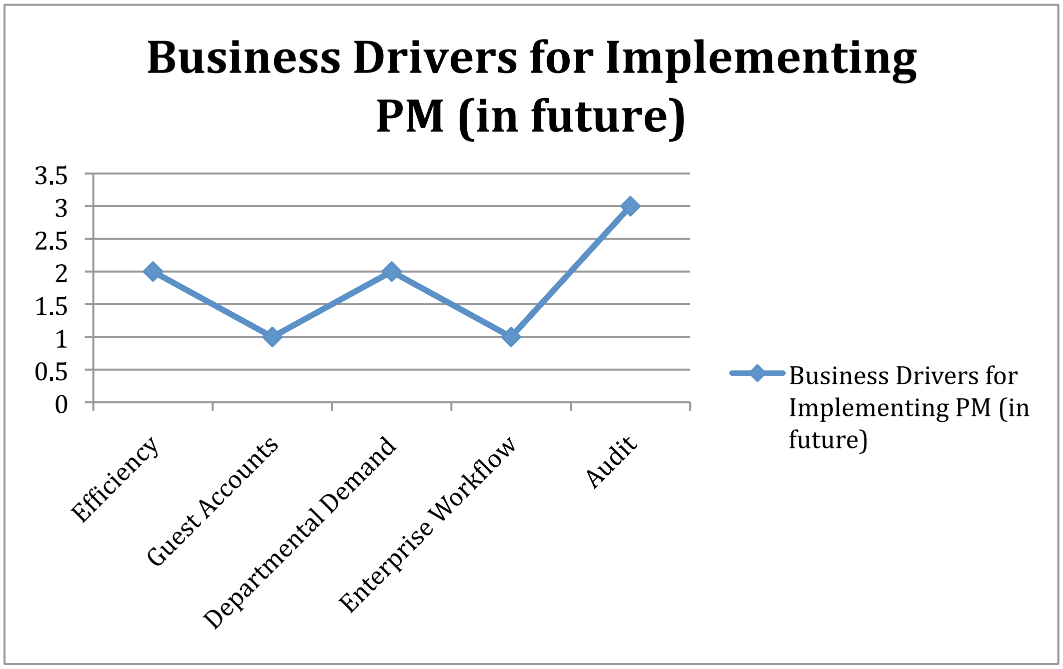
Automated policy or "rule" management was slightly more widely employed among responding sites than privilege management tools, with some 31% of responders (split roughly equally between public and private institutions) indicating that their sites used some form of policy management.

On the whole, these responses seem to confirm the hypothesis that sites often start with the deployment of centralized identity management facilities and later deploy services that depend upon those facilities, including group management and, ultimately, privilege management. Most responding schools indicated that they have in place the basic necessities for taking advantage of some form of centralized privilege management, but most have not yet made inroads into this space.

More Specific Privilege Management Questions

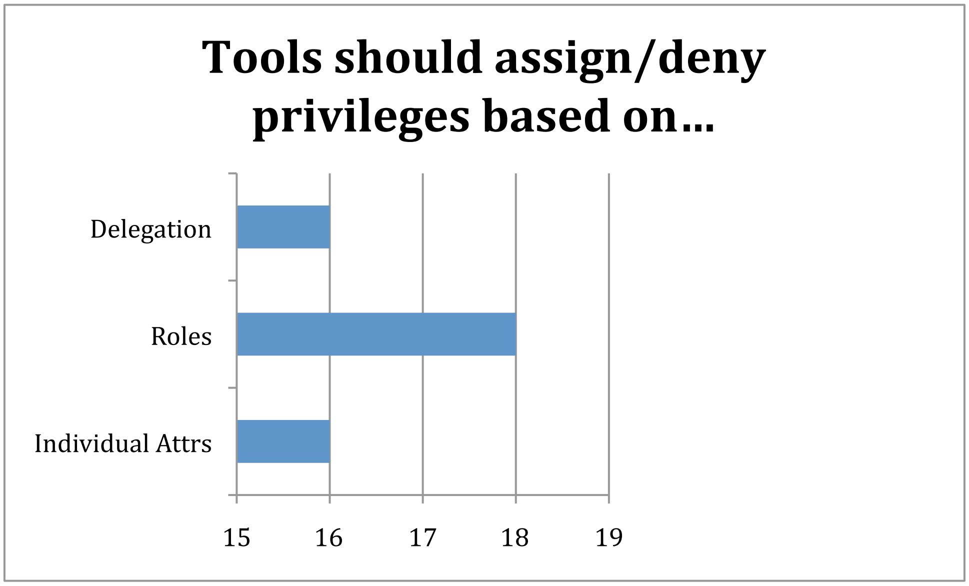


The sites that indicated they were employing some form of centralized privilege management were further asked to describe how well their existing deployments meet their current and expected future needs. 38% of respondents reported that they had current needs that were not met by their existing solutions, while another 37% indicated that their existing solution meets their current needs but is expected to fall short of their projected needs for the future. Only 25% of respondents reported satisfaction with their existing privilege management tools as answers to both their current and their anticipated future needs.



The survey went on to ask those sites not currently employing any form of centralized privilege management whether they had plans to deploy some form of privilege management in the next 12 months, and what the primary business drivers for such a deployment at their sites might be. Responses to this question were mixed. Three respondents indicated that audit requirements were a significant business driver for their sites; two each indicated that efficiency and the needs of distributed departments for better privilege management options were significant drivers for their sites, and one each listed the management of guest privileges and support for enterprise workflow patterns as significant drivers for their privilege management decisions.

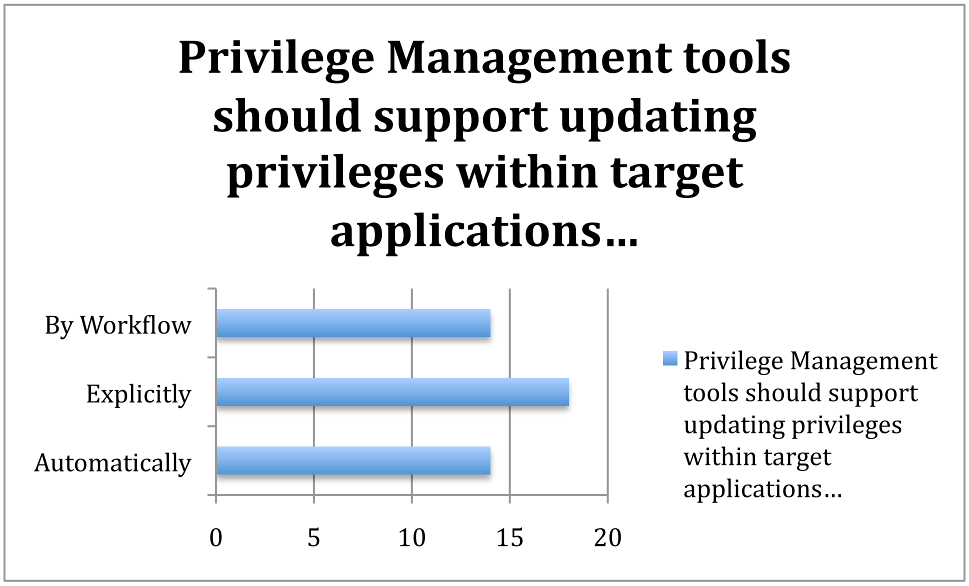
Combined, these results suggest that there is substantial unmet demand for better privilege management facilities within the community, and that facilities capable of solving a few key problems – audit requirements, the need for greater process efficiency, and support for distributed management – could go a long way toward meeting those needs.



In discussions with the Signet development group, it became clear that one topic on which opinions differ within the privilege management space is the mechanism by which privileging systems should make privileging decisions.

The survey asked respondents to indicate which of three approaches would be appropriate in their environments – assigning privileges based on explicitly conveyed, individual attributes (eg., if an individual's identity information includes a "BuildingTwelveAccess" attribute, the individual will be provisioned with door access to Building #12), assigning privileges based on roles (eg. a collection of Privileges pertaining to grant management may be grouped together and assigned to individuals when they take on the role of "principal investigator", or when individuals are added to a "PI" group), and assigning privileges based on delegations (eg., the Dean of Faculty is authorized to designate who among the faculty should have access to the faculty lounge, and access is either granted or denied based on explicit delegation by the Dean).

Respondents were unanimous in their support for some form of role- or group-based privilege management – all 18 respondents indicated that role- or group-based assignment of privileges should be supported, citing primarily employee-related scenarios (in which employees receive privileges based on their job roles). Almost 90% further agreed that both delegation and individual attribute-based privilege assignment should also be supported. Both delegation and attribute-based privilege assignment were largely identified as solutions for exceptions or for cases in which political pressures or sensitivities might make role- or group-based privileging decisions too complicated to automate.



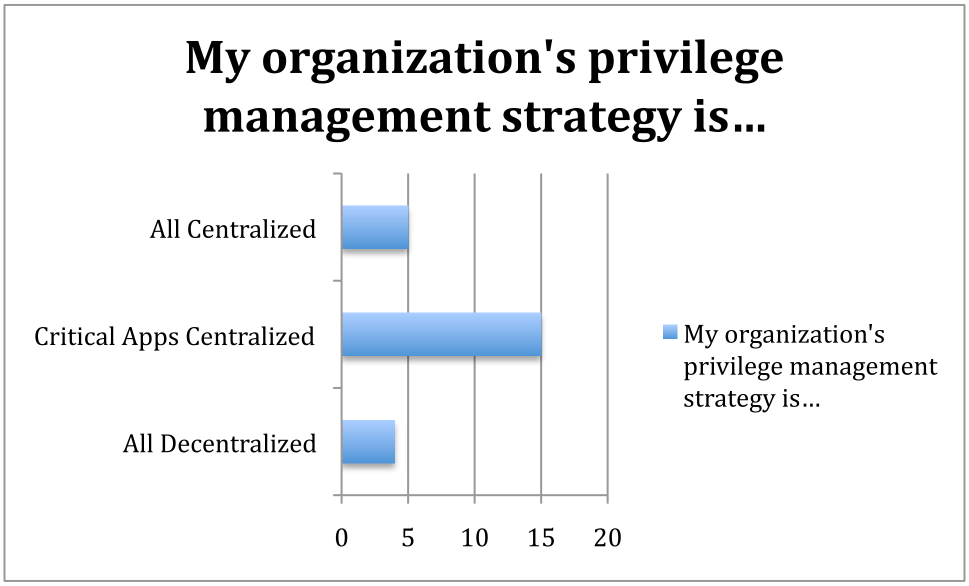
Respondents were additionally asked a series of questions focusing on the ways in which they expect privilege management should be deployed within their organizations, and the ways in which they would expect privilege management facilities to interoperate with existing applications and systems within their institutions. 100% (18 out of 18) of the responding sites indicated that they would expect a privilege management facility to support explicit, manual updating of privileges within target applications. 77% (14 out of 18) indicated that tools should support the use of workflows involving approvals or other forms of human intervention to trigger the application of privileges to target systems and applications. A similar 77% indicated that they would expect privilege management tools to support some form of automatic, unattended application of privileges.

Asked to provide scenarios under which each of the updating methodologies above might be applicable, respondents offered a wide variety of suggestions.

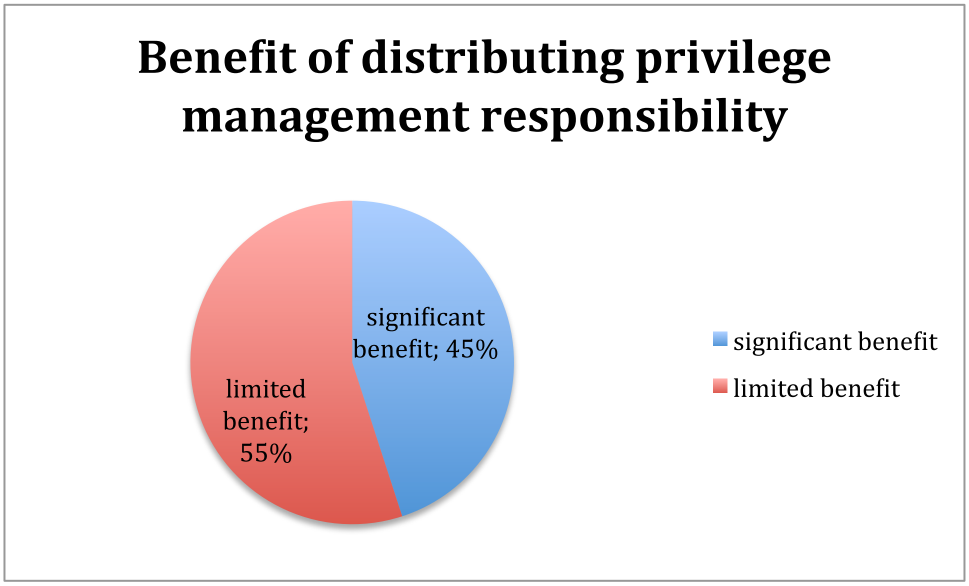
Those providing scenarios for automatic update of privileges focused on three basic cases – an "onboarding" case (in which certain basic privileges are assigned based upon a new subject's affiliation, like faculty access to a faculty lounge), an "offboarding" case (where an employee or student separates from the institution and has her privileges removed automatically), and an "organizational change" case, in which changes in organizational structure lead to privileges being updated automatically to reflect individuals' new relationships with one another and the organization. By far the most commonly cited case was the "offboarding" case, suggesting that privilege management tools may be widely seen as useful for addressing security issues pertaining to stale authorization data.

Those providing scenarios for explicit manual update of privileges focused on two basic cases – exception handling (in which some human actor with a high level of privilege needs to activate an exception to some automatic rules or policy, either adding or removing a privilege from someone by fiat) and security handling (in which a security issue, eg.., the forcible separation of an employee from the institution, leads to a need to guarantee immediate removal of privileges without waiting for automatic updates to occur).

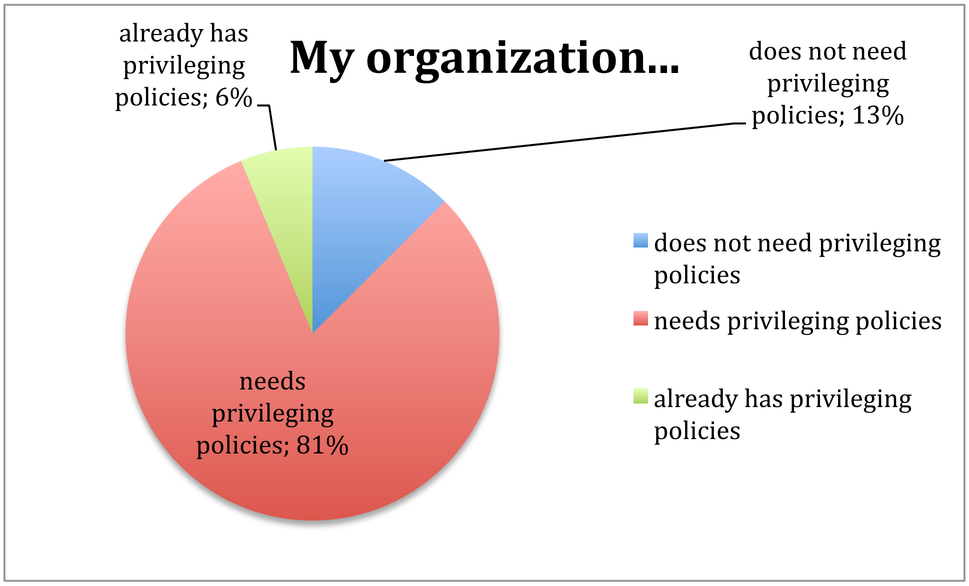
Scenarios offered for the use of workflow were more varied, but all centered on a single basic case in which some privilege, set of privileges, or role requires a complex set of one or more approvals in order to be assigned to an individual.



Respondents were asked to characterize their organization's current or preferred privilege management strategy as one of "fully centralized", "centralized for critical applications but decentralized for other applications", or "fully decentralized". The responses are shown above – of the 24 organizations providing responses to the question, 15 indicated that their strategy involves centralizing privilege management for their critical applications, and another five indicated that their strategy involves centralizing all privilege management. Only four of the respondents indicated that their privilege management is fully distributed.



In follow up, sites were asked to gauge the extent to which granular delegation of privilege management authority and responsibility to agents with direct knowledge of specific application areas and/or specific sub-organizations would yield benefits for their organizations. Respondents could choose one of three responses – significant benefit (with the expectation that departmental privilege managers would be better able to make good privileging decisions than managers in central IT), limited benefit (due to policy or political realities which would impede full distribution of this authority to departmental agents), or no benefit at all (due to the expectation that departmental privilege managers either could not or would not make good privileging decisions). No sites chose the latter option; sites were split 55%/45% between choosing the "limited benefit" and the "significant benefit" option. Coupled with the responses to the previous question, it would appear that even in the most fully centralized of organizations, distribution of privileging authority and responsibility can be expected to offer benefits over full centralization of privileging authority.



As a final gauge of the strategic position of responding organizations, the survey asked respondents to indicate whether their organization already has in place policies to control the assignment and removal of privileges, needs but does not currently have policies on privilege assignment and removal, or does not need to express policy in the area of privileging. The results, shown above, so that almost 90% of responding organizations expect that some form of policy is required to manage privileges in their environments, while only a small fraction (6%) believe that they have sufficiently articulated policies in this area. While policy management was not strictly the focus of the survey, responses to this question suggest that many sites could benefit from stronger policies on which to base privileging decisions.

Free Response Questions

The functional section of the survey closed with a set of free-response questions asking respondents to identify what they believed to be the most important features of an effective privilege management system and the three biggest issues they would expect to see more effective privilege management tools address within their organizations. Not unexpectedly, answers to these questions varied widely from respondent to respondent, but a few basic themes arose from each.

In response to the question of what the most important features of a successful privilege management solution might be, the most common themes were:

- Ease of use for end-users and "line of business" users.
- Adherence to standards, APIs, and ease of integration with applications
- Auditing and logging of privileging decisions and actions; transparency

- Security, especially effective deprovisioning of privileges when individuals separate from the organization or change roles

Notable additional points raised by one or more respondents in answering this question included:

- Providing patterns for well-known use cases to simplify use by less technical privilege managers
- Separating authentication (AuthN) from authorization (AuthZ)
- Scoping privilege based on organizational boundaries (so that wide privileges can be assigned to individuals only within narrow boundaries)
- 3-part authorization semantics (granting rights to a *person* to perform a *function* on a particular *target*)
- Flexibility to support both live privilege look-up and batch-mode privilege application to cooperating applications
- Qualification of privilege (eg., "only on weekdays" or "only after completing safety training")

Responses to the question of what problems or issues might be solved by the deployment of more effective privilege management followed similar lines, with the most common themes being:

- Slow or inaccurate onboarding of new hires/new affiliates
- Slow or inaccurate offboarding of separated individuals
- Security and the so-called "privilege snowball"
- Auditability and transparency of privilege management

Some additional issues identified as likely to be addressed by enhanced privilege management tools included:

- Guest account privilege management
- Efficiency of operation
- Decentralization of access control information

One respondent, with a background in auditing, offered a somewhat different point of view. Rather than identify issues likely to be addressed if better privilege management tools could be deployed, the respondent identified a set of prerequisites for enhancing privilege management that may, in many cases, not be currently met within organizations. These were:

- Data Classification
- Policy Development
- Risk Assessment

It is worth noting that other sites indicated, either explicitly or implicitly, that some of these issues might pertain to their situations, as well.

Technical Questions

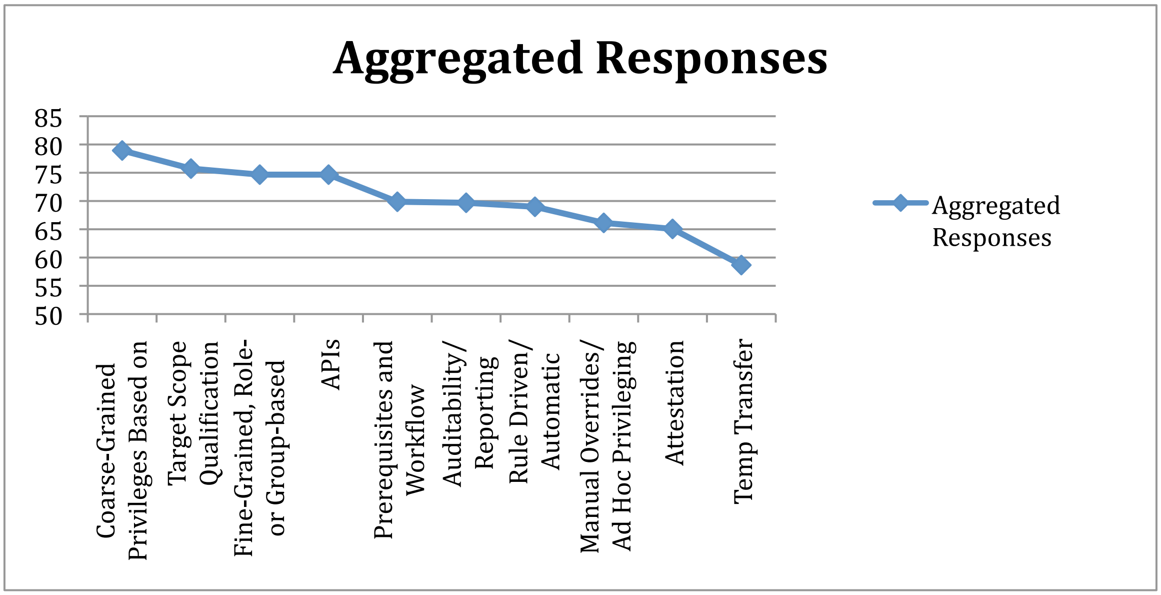
Overall results

The final section of the survey comprised a set of 21 Likert scale questions intended to gauge the degree of interest in or need for specific technical features in privilege management solutions. Of the original 25 responding sites, only 16 provided responses to this more technical portion of the survey. The 21 questions covered 10 focus areas (with some questions covering more than one focus area, and some focus areas being addressed by multiple questions).

In the Likert questions, respondents were asked to indicate their level of agreement with specific statements using a five-point scale, with the five points interpreted as:

1 – Strongly Disagree
2 – Mildly Disagree
3 – Neither Agree nor Disagree
4 – Mildly Agree
5 – Strongly Agree

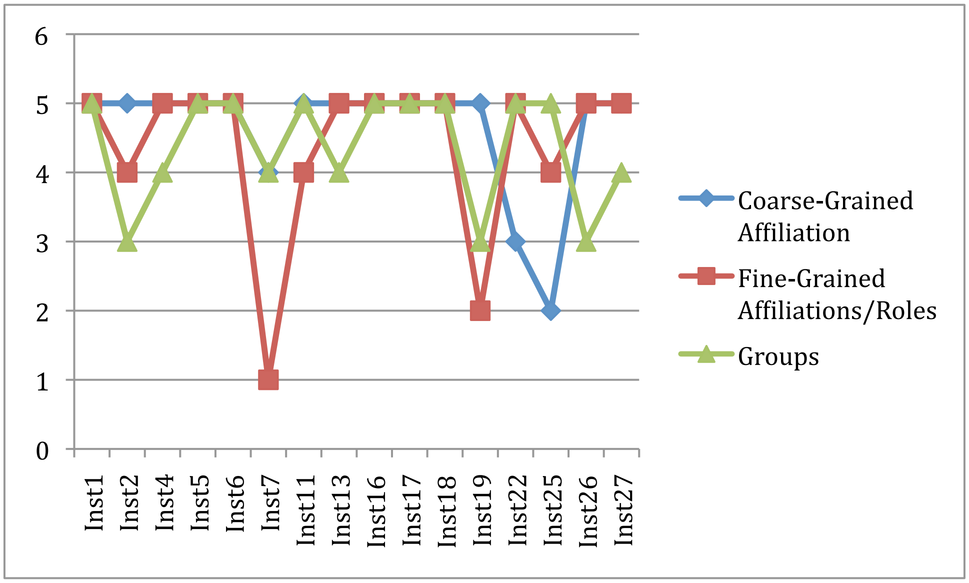
The aggregated Likert responses are depicted in the chart below.



Interim results presented at the October, 2008 Internet2 Member Meeting showed that the most widely-agreed-upon technical requirement for an effective privilege management facility was the availability of usable APIs, with automatic privilege assignment and reporting or auditing running a close second and third. As depicted in the above chart, after the addition of responses from a wider audience, the overall picture changed – the three most widely-agreed-upon technical requirements became support for coarse-grained privilege assignment based on broad affiliations, scoping of privileges based on target identities, and support for fine-grained role-based and group-based privilege assignment. This suggests that the perceived technical needs of organizations may be different depending on their history with privilege management – sites participating in the Signet working group expressed a qualitatively different set of needs than others.

Sources of Privileging Information

One axis along which privilege management approaches vary is the means by which privileges are derived – what information or attributes are significant in the calculation of whether an individual should be granted a particular privilege or whether an individual's privileges should change because of some change in the individual's attributes or roles.



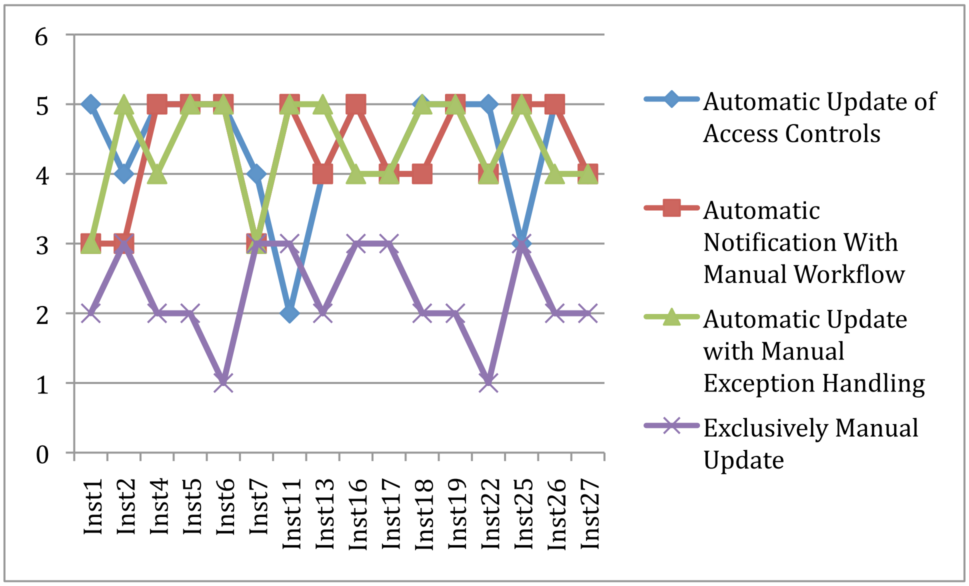
To gather information about the methods the community is using or would like to use to make privileging determinations, three survey questions asked respondents to indicate their level of agreement with the statements "Our privilege management tools need...:"

- ...the ability to make privileging decisions based on broad classes of affiliation ("employee", "student", "faculty", etc.)
- ...the ability to make privileging decisions based on fine-grained roles or affiliations ("CS undergraduate", "HR manager", "Medical School faculty")
- ...the ability to make privileging decisions based on membership in derived or ad hoc groups (eg. "Prof. Smith's graduate students", "Project X team members")

Responses to these questions are outlined in the chart above. With few exceptions, respondents felt that the ability to make privileging decisions based on broad affiliation classes was important. Group-based privileging and privileging based on fine-grained roles was somewhat less important to respondents, on average, than basic, coarse-grained privileging based on broad affiliations.

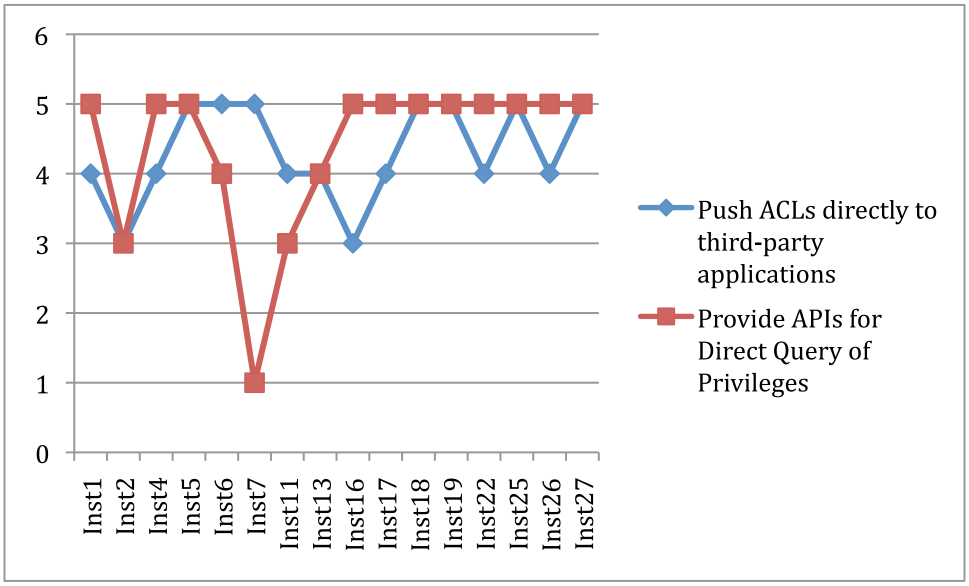
Privilege Assignment

Another area of difference between privilege management implementations is the means by which privileging decisions made by or recorded in the privilege management system take effect – how privileges defined and managed in the system are translated into access control decisions on the part of other systems and applications. Differences arise along two distinct continuums – what might be characterized as "push" versus "pull (whether privilege management facilities trigger or perform updates of ACLs within other applications, or whether other applications consult privilege management facilities as needed to make their access control decisions), and what might be characterized as "automatic" versus "prompted" (whether changes in the state of individuals, rules, or roles automatically effect changes in access controls, or whether some human intervention is required to activate changes in access controls).



The chart above depicts the answers provided by respondents to Likert questions focusing on four distinct points along the latter continuum, between fully automatic update of access controls based on privilege calculations and entirely manual update of access controls. With only two exceptions, all respondents agreed more strongly with statements indicating a need for some form of automatic privilege assignment (possibly including workflows or some other manual intervention for exceptional cases) than the statement indicating that their sites would need no such automation and would be better served by manual access control management.

Similarly, the chart below depicts the answers provided by respondents to Likert questions focusing on the two poles of the former continuum – between "push" and "pull" models for privilege distribution.

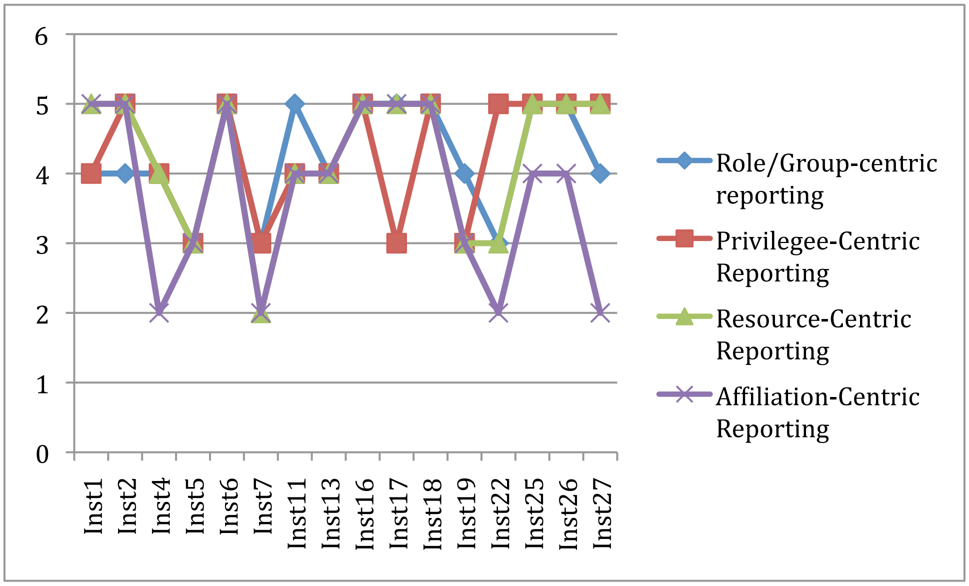


As the chart depicts, most respondents showed a much stronger affinity for the API-based "pull" model of privilege distribution, although there was some dissent (one respondent actively disagreed with the proposition). There was no active disagreement with the premise that privilege management services should support the "push" model, but support for the premise was weaker in most cases.

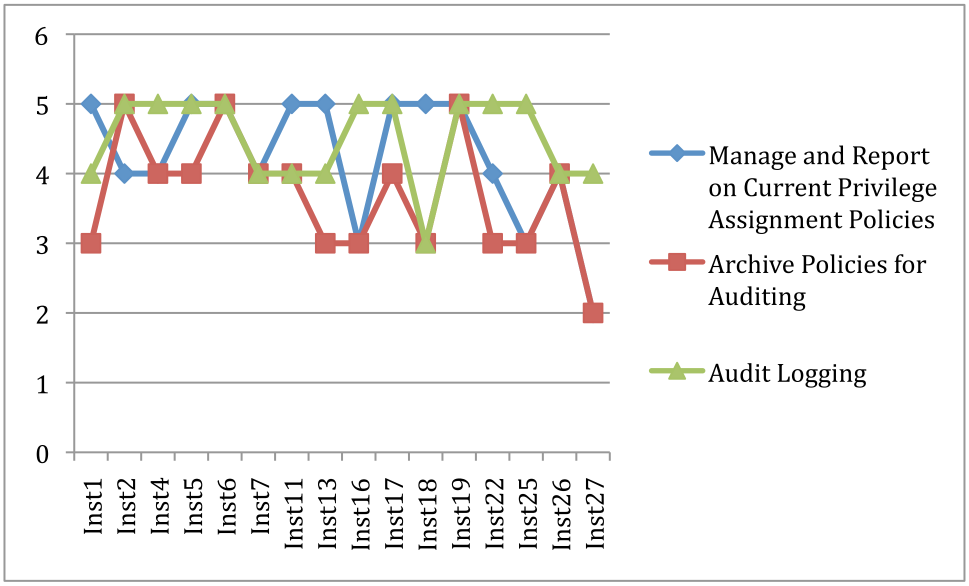
Audit and Reporting

Whether welcome or unwelcome, discussions of privileges and privilege management inevitably attract the attention of security and audit groups, and for good reason – privilege management, perhaps more so than any other component of identity management, directly addresses basic security issues of interest to both groups.

The survey included a set of questions focusing on the kinds and characteristics of reporting and audit logging respondents might need in a privilege management facility. The charts below depict the responses to those questions:



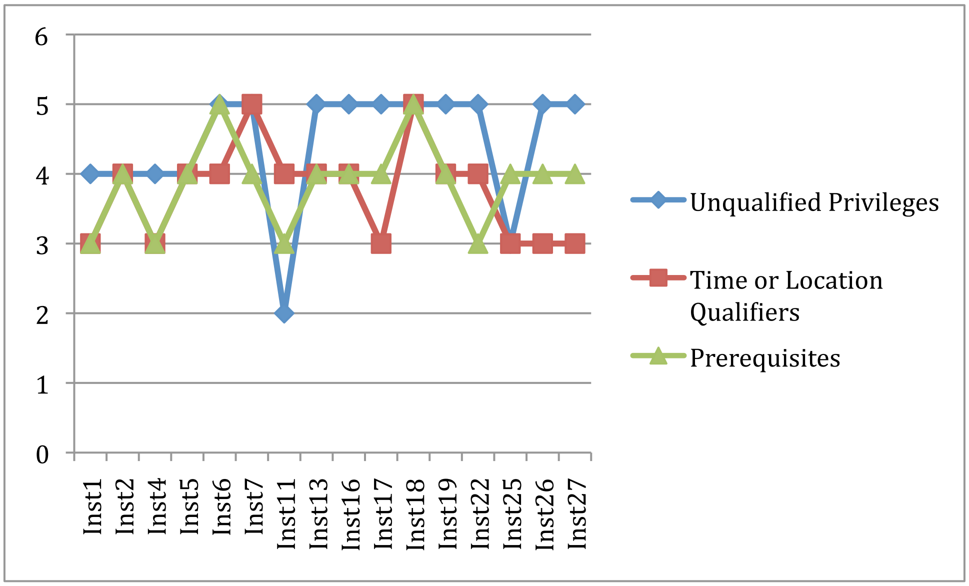
One set of questions explored the types of reporting that respondents expected to be important in their organizations. In the graph above, respondents' reactions to statements about the four approaches to reporting explored in the survey are outlined. Individuated reports – reports of privileges assigned to individual privilegees (answering questions like "what privileges does Prof. Smith hold?") and privileges targeting specific resources (answering questions like "Who has the ability to change Gina's declared major") were considered more important than aggregate reports (answering questions like "What privileges are held by payroll clerks?", or "What privileges are afforded faculty in the Sociology Department?"). Among the respondents, no one disagreed with statements indicating a need for any of the individuated reports, while a number of respondents indicated mild disagreement with statements indicating a need for aggregate reporting.



A second set of questions explored the extent to which historical auditing of privileging systems might be of importance to respondents – those three questions are depicted in the chart above. There was almost unanimous agreement that some form of audit logging should be supported by privilege management facilities. Respondents were less concerned about the need to for reporting of privilege management policies, and even less concerned about needs around the archiving of policy information for historical auditing purposes.

Privilege Qualification

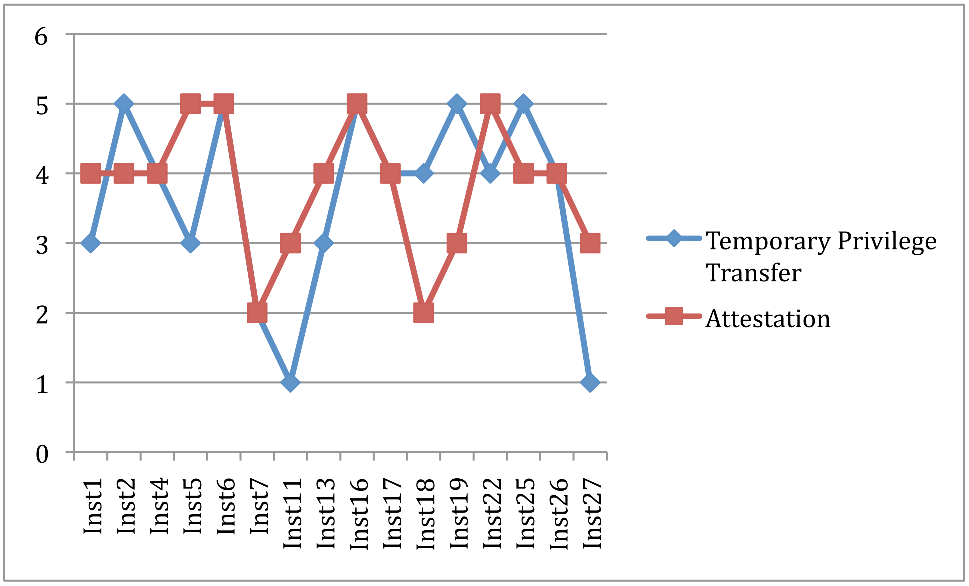
Some privilege management models presuppose that privileges are entirely unqualified – that privileging decisions should be made based solely on the identity of the actor. More commonly, privilege management models include three components -- the actor, the target, and the operation being performed in their privilege calculations, but ignore time, space, or other factors. Other privilege management models include general qualifiers of privilege – time of day or year, physical location of the actor, etc. Some models likewise support the consideration of prerequisites in privilege calculation. The survey included three questions designed to explore respondents' attitudes toward privilege qualification features in privilege management facilities. The results appear in the chart below:



Not surprisingly, most respondents felt strongly that privilege management facilities would need to support the use of unqualified privileges. Prerequisites for privilege (eg., in support of scenarios like "as an electrical technician, Gina is authorized to use the electrical shop's departmental minivan only if her driving safety test results are current and satisfactory") were slightly more important to respondents on the whole than time- and location-based privilege qualifications (eg., "as an employee in the Registrar's office, Tom can access undergraduate registration records online between the hours of 7am and 5pm on weekdays", or "Dr. Smith may view patient blood test results online, but only when working from a computer inside the medical campus").

Miscellaneous Features

Two features not easily connected with any of the feature groups outlined above were also addressed by the survey – privilege transfer and privilege attestation. Privilege transfer features allow the holder of a privilege (the privilege grantee) to temporarily transfer his or her privilege to another individual, usually for purposes of business continuity or coverage during absences. A typical example might be a Dean who is taking a three week cruise in the Mediterranean and will be unable to authorize student leaves of absence transferring that privilege to an Assistant Dean for the duration of her vacation. Attestation features allow for a specific type of workflow process wherein privilege grantors may be periodically required to revalidate or "attest to" the privileges they have granted to grantees. A typical example might be a faculty member being required every six months to reassert through some automated system the privileges he has granted to a colleague's graduate students within a learning management system. The chart below depicts the responses to these two questions:



As the chart shows, responses to these two questions varied widely. Eleven respondents agreed to some extent that attestation features would be important in their environments, and ten agreed that temporary privilege transfer features would be important. In both cases, two respondents indicated that each would not be important.

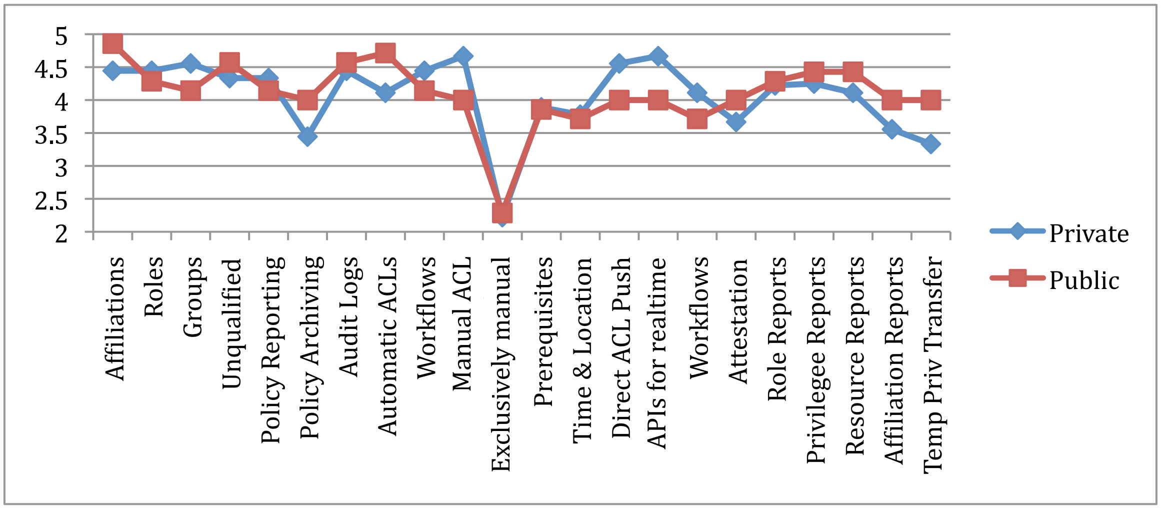
Additional Trends

One desired outcome from the privilege management survey was to identify what, if any, trends might exist in the expressed needs or preferred strategies for addressing privilege management within a few broad subsets of the higher education community. Do, for example, private institutions show more affinity for distributed privileging models than public institutions, or vice versa?

Combining institutional demographic data collected early in the survey with Likert results from the technical section of the survey may shed some light on whether and how organizational demographics related to respondents' choices in answering the survey.

Public versus Private Organizations

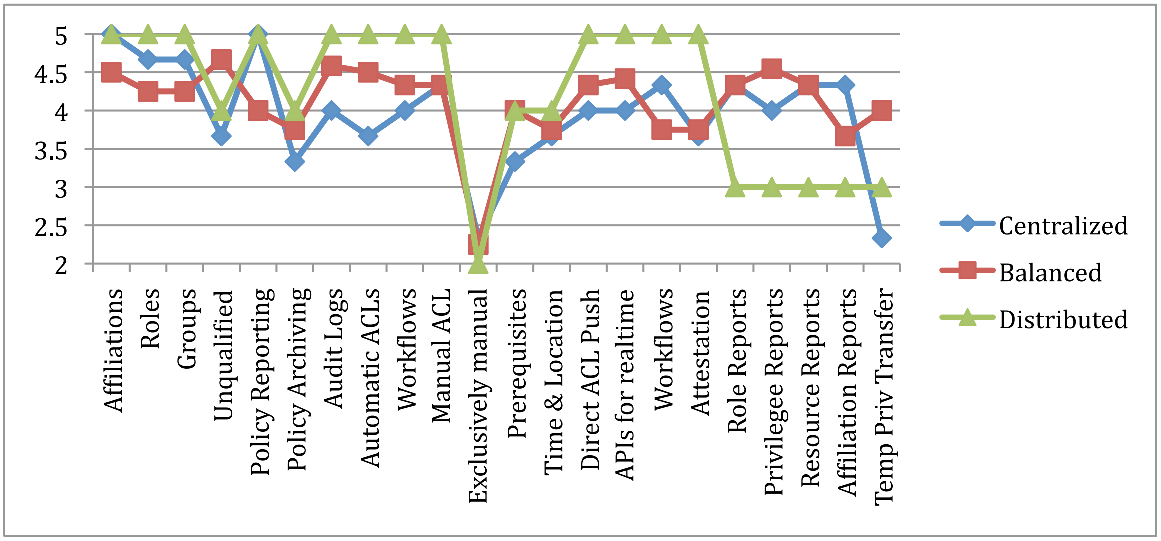
The chart below depicts the averaged Likert responses from organizations self-identified as either public or private:



As the chart shows, overall variance between public and private institutional responses was low, but some trends do emerge. Public institutions appear to be more concerned with auditing and reporting features, as evidenced by responses to questions about reporting features and about audit logging and policy retention. Private institutions, on the other hand, appear more concerned with automation (as evidenced by responses to questions about APIs, workflow, and automatic ACL propagation) and granularity of control (as evidenced by responses to questions about manual overrides and group- and role-based privilege assignment).

Centralized versus Distributed IT Environments

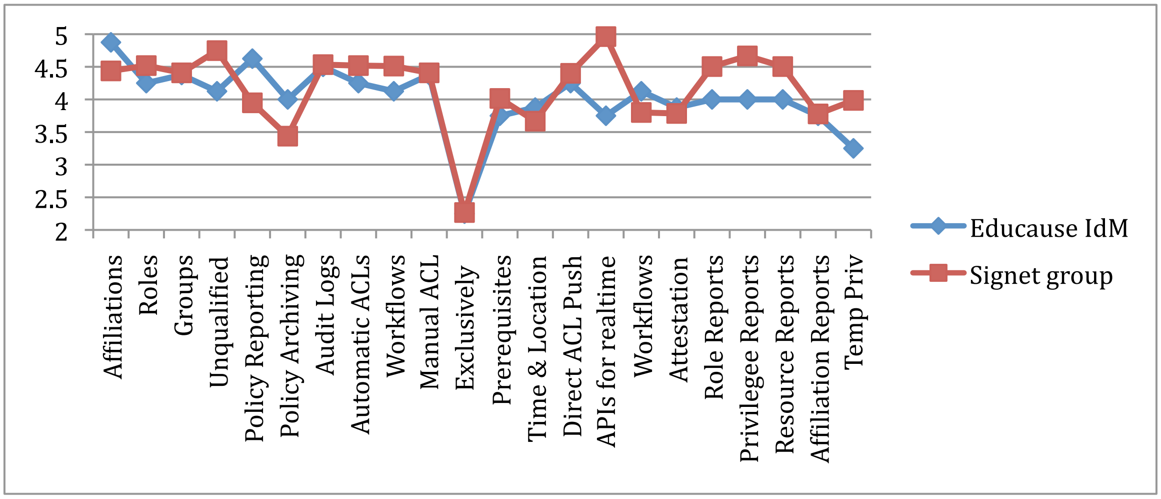
Another axis along which respondents differed was the degree of centralization of their overall IT environments. The chart below depicts the average Likert responses from organizations self-identifying as either “mostly centralized”, “roughly balanced between centralized and distributed”, or “distributed”:



Sites reporting their overall IT environment as primarily “distributed” in nature demonstrated noticeably less concern than other sites about reporting features, but the same or more concern about audit logging and policy tracking. They indicated more interest in automation and workflow (including attestation) than their more centralized counterparts.

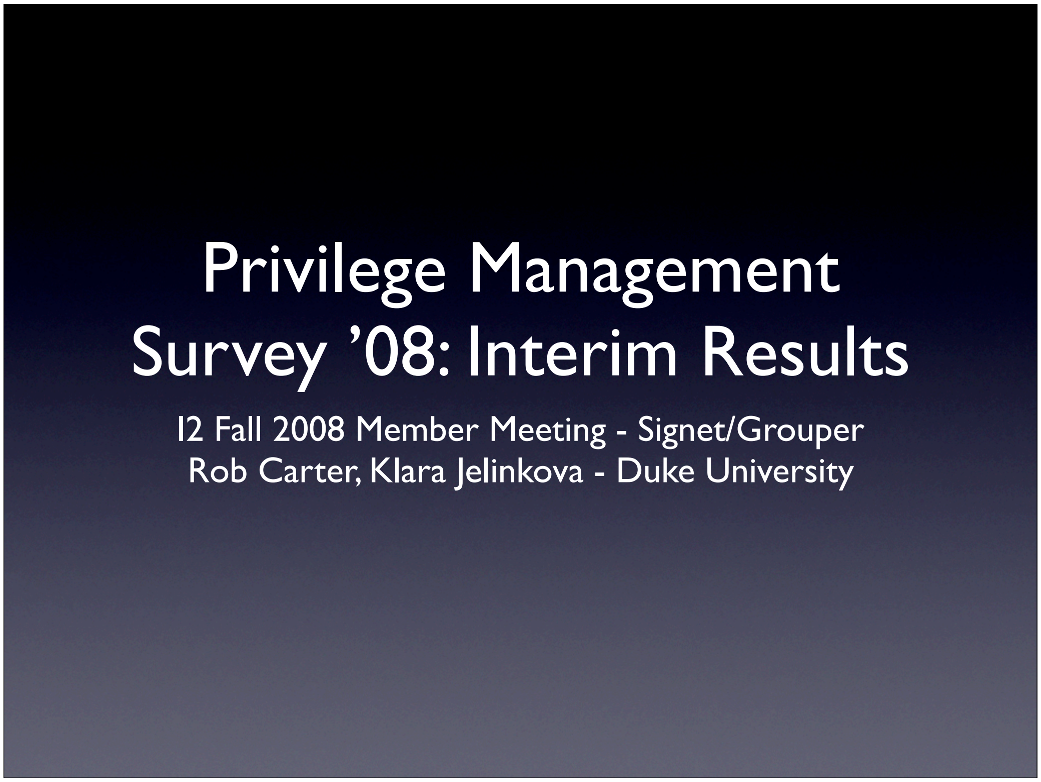
Signet Participation

As noted at the start of this report, the survey was administered to two distinct collections of sites at different times – one set of respondents comprised organizations involved in one or another fashion with the Signet effort while the other was a somewhat broader collection of organizations participating in the Educause IdM interest group. The averaged Likert responses from organizations in those two categories are depicted in the chart below:



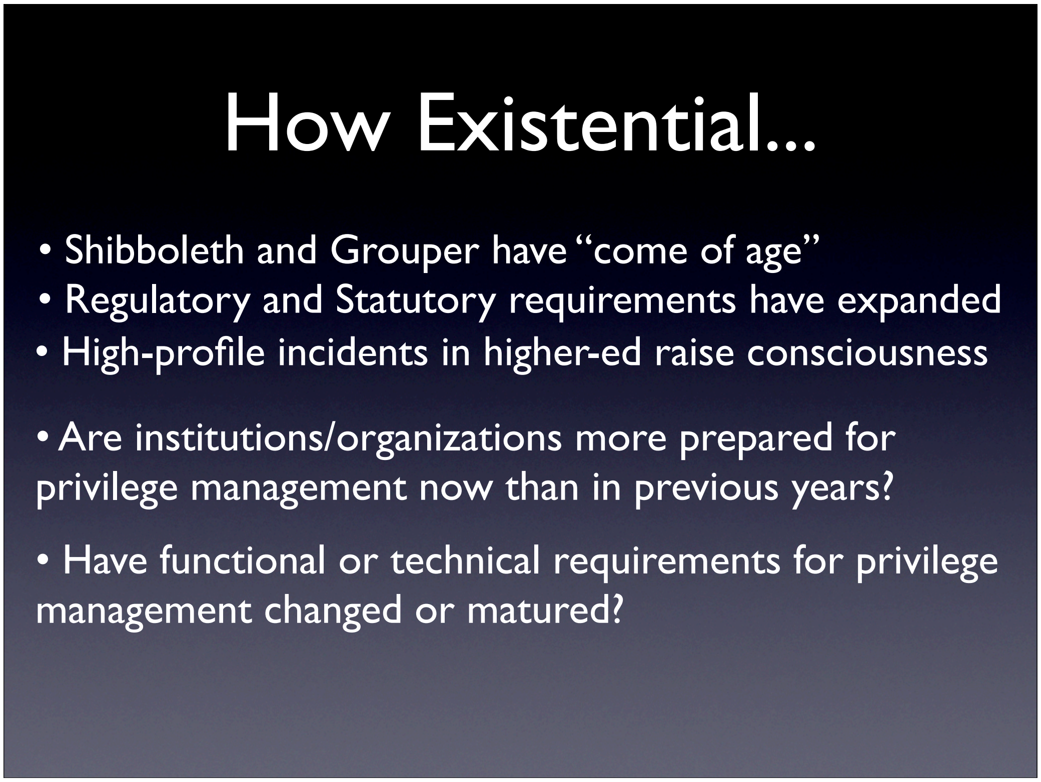
Signet participants responding to the survey were somewhat more likely to consider reporting and automation features important and somewhat less likely to consider policy tracking an workflows important than their colleagues within the Educause group. Interestingly, Signet participants in the early round of the survey considered APIs extremely important, while non-Signet participants in the latter rounds of the survey considered APIS comparatively unimportant, on average. Whether this disparity reflects differences in the extent to which different sites have already put effort and consideration into privilege management tools or some other factor is not clear from the results of the current survey.

Appendix A: Interim Results (Fall, 2008 I2 Member Meeting Presentation)



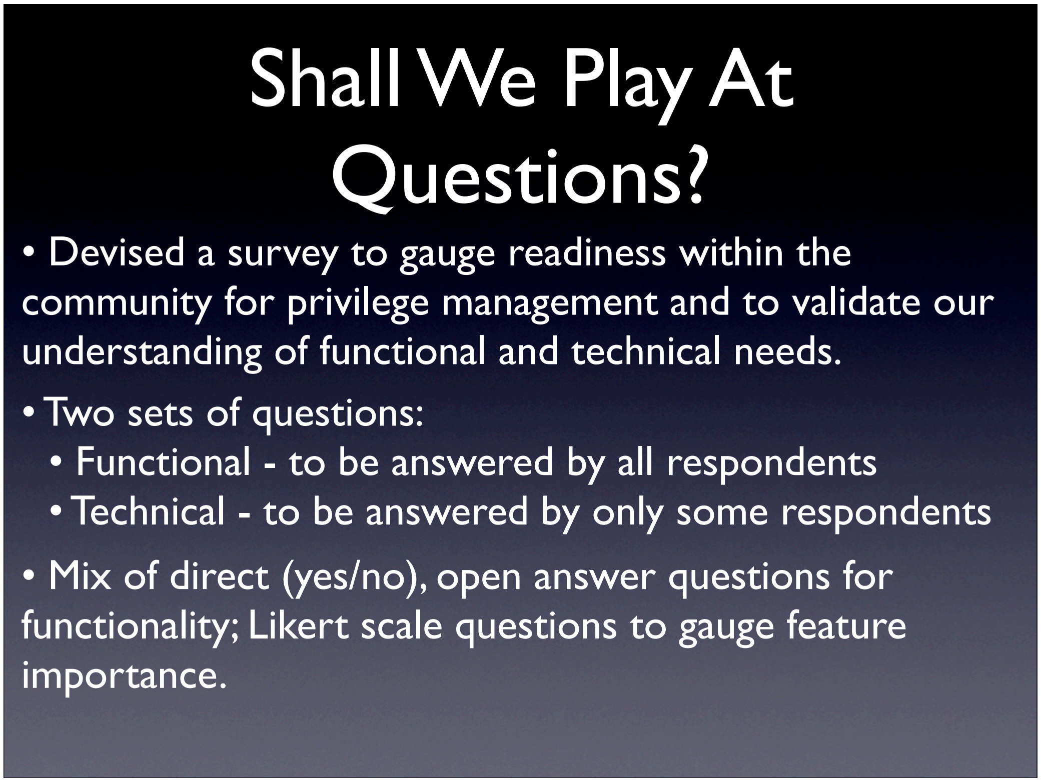
Privilege Management Survey '08: Interim Results

I2 Fall 2008 Member Meeting - Signet/Grouper
Rob Carter, Klara Jelinkova - Duke University



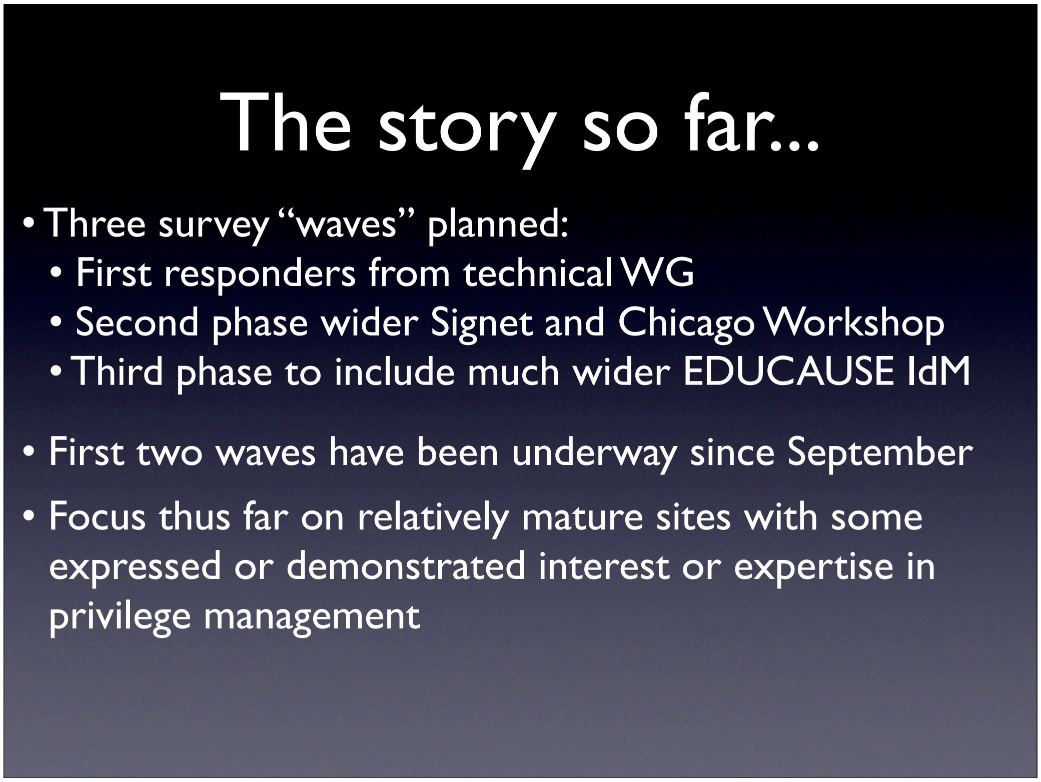
How Existential...

- Shibboleth and Grouper have “come of age”
- Regulatory and Statutory requirements have expanded
- High-profile incidents in higher-ed raise consciousness
- Are institutions/organizations more prepared for privilege management now than in previous years?
- Have functional or technical requirements for privilege management changed or matured?



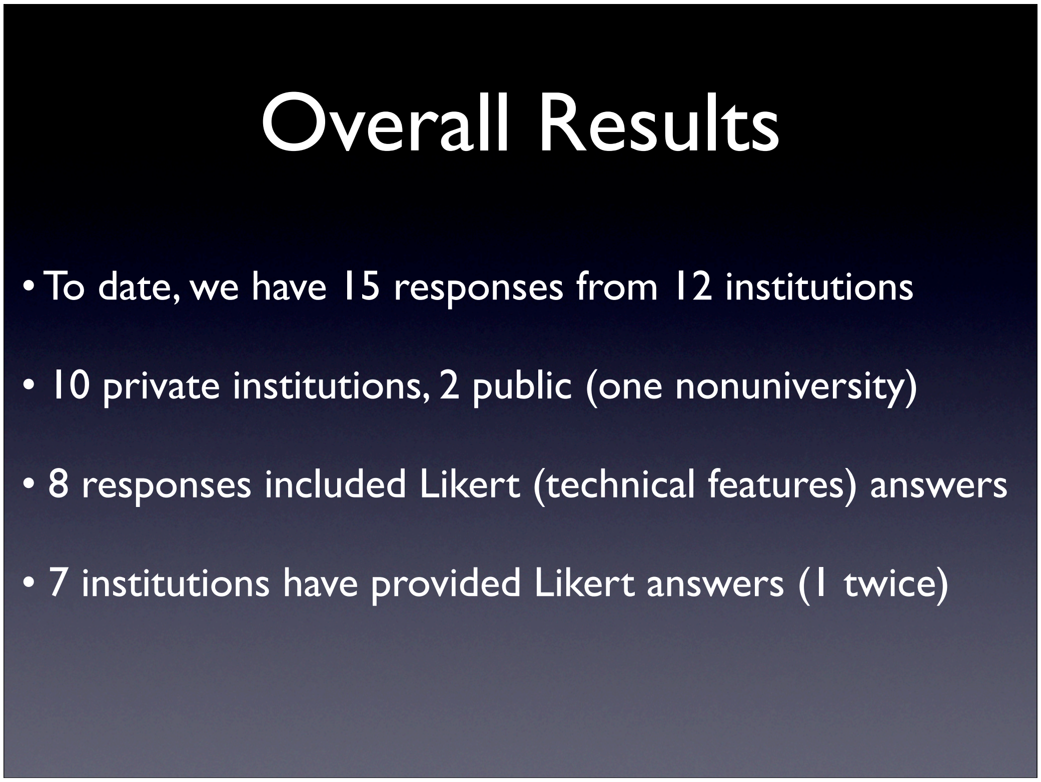
Shall We Play At Questions?

- Devised a survey to gauge readiness within the community for privilege management and to validate our understanding of functional and technical needs.
- Two sets of questions:
  - Functional - to be answered by all respondents
  - Technical - to be answered by only some respondents
- Mix of direct (yes/no), open answer questions for functionality; Likert scale questions to gauge feature importance.



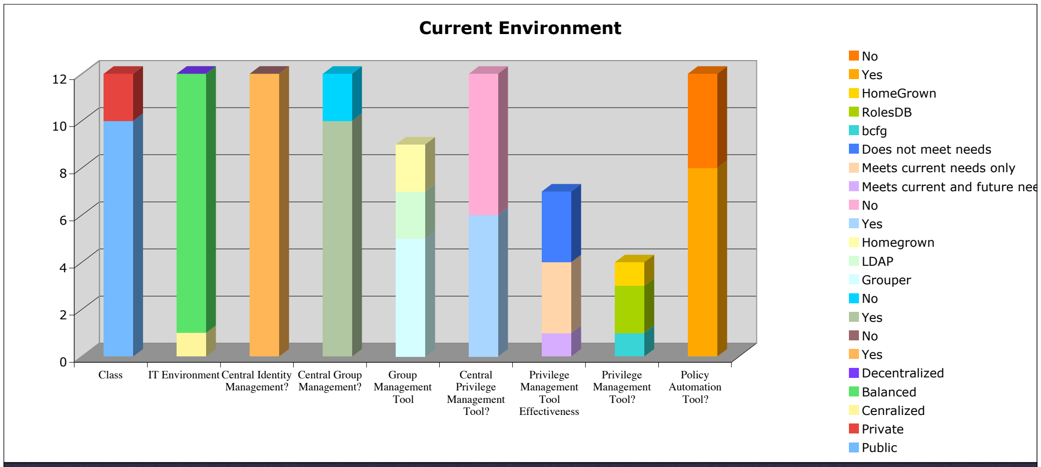
The story so far...

- Three survey “waves” planned:
  - First responders from technical WG
  - Second phase wider Signet and Chicago Workshop
  - Third phase to include much wider EDUCAUSE IdM
- First two waves have been underway since September
- Focus thus far on relatively mature sites with some expressed or demonstrated interest or expertise in privilege management

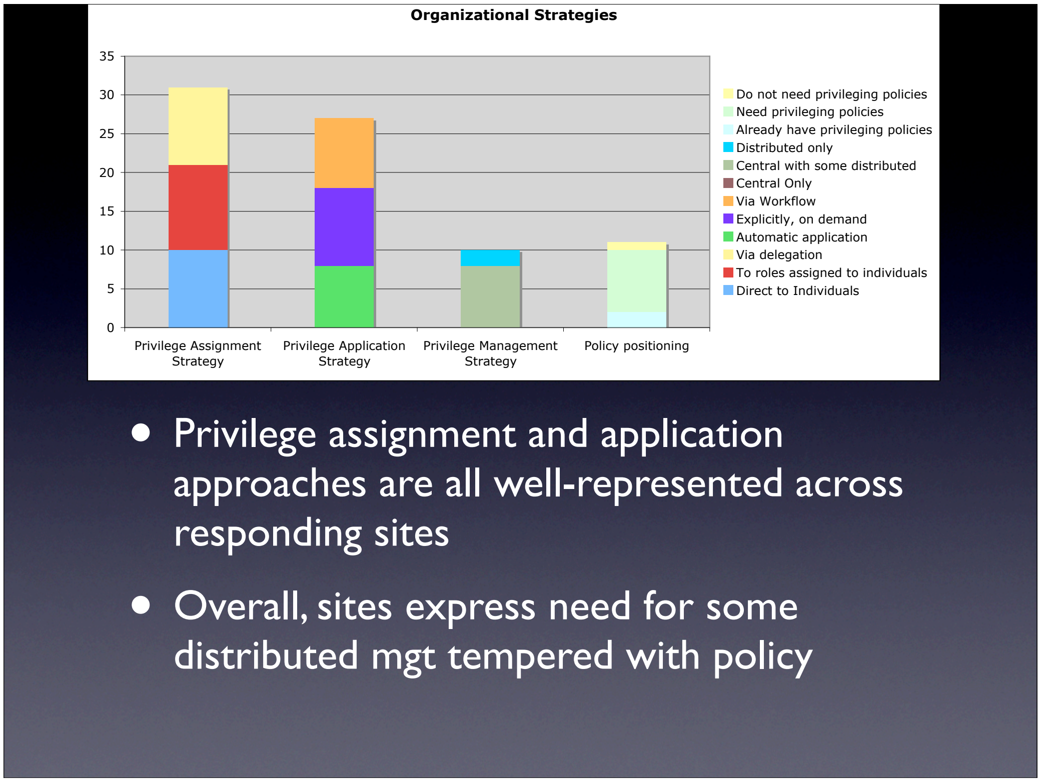


Overall Results

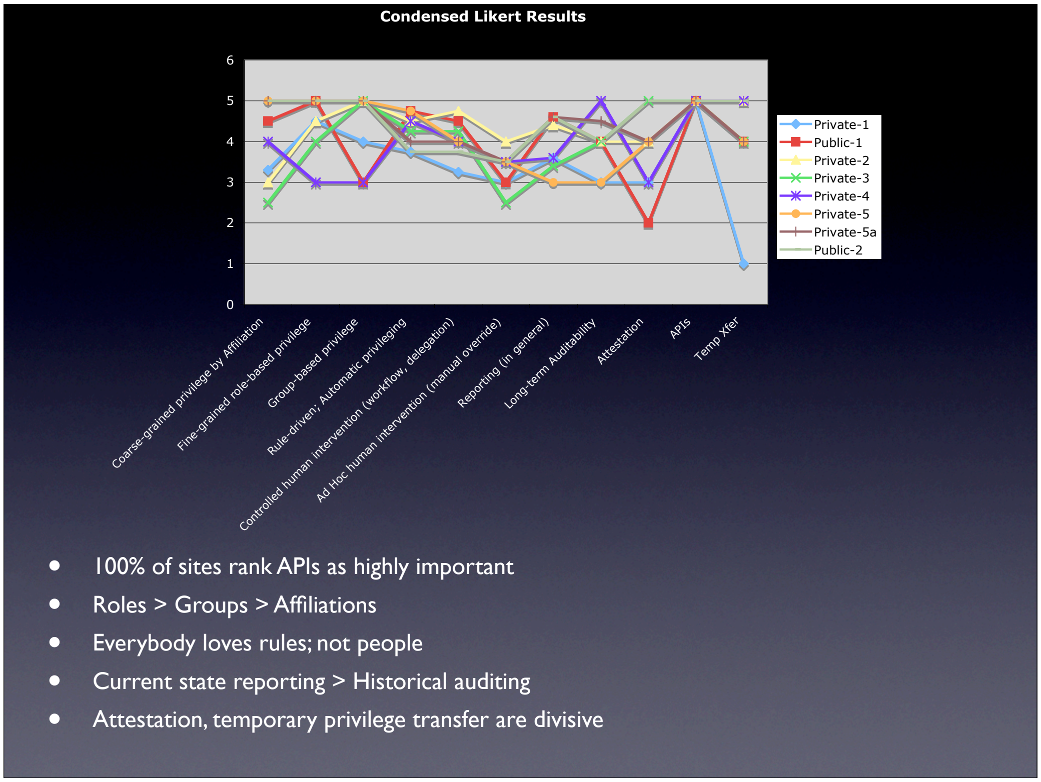
- To date, we have 15 responses from 12 institutions
- 10 private institutions, 2 public (one nonuniversity)
- 8 responses included Likert (technical features) answers
- 7 institutions have provided Likert answers (1 twice)



- 100% of responding sites employ central IdM
- 83% employ central group management
- 67% use some form of policy automation
- 50% of responding sites employ central privilege mgt...
- ...but only 14% believe their current solution will last...
- ...and 43% are not currently satisfied with their solution

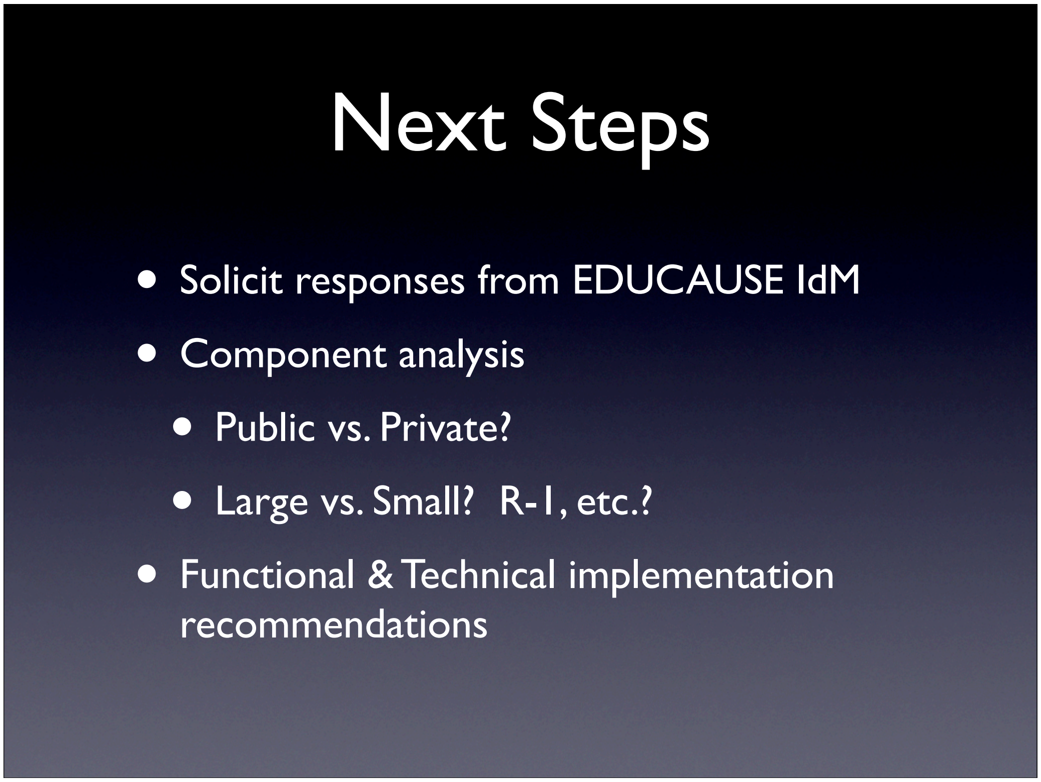


- Privilege assignment and application approaches are all well-represented across responding sites
- Overall, sites express need for some distributed mgt tempered with policy



Condensed Likert Results

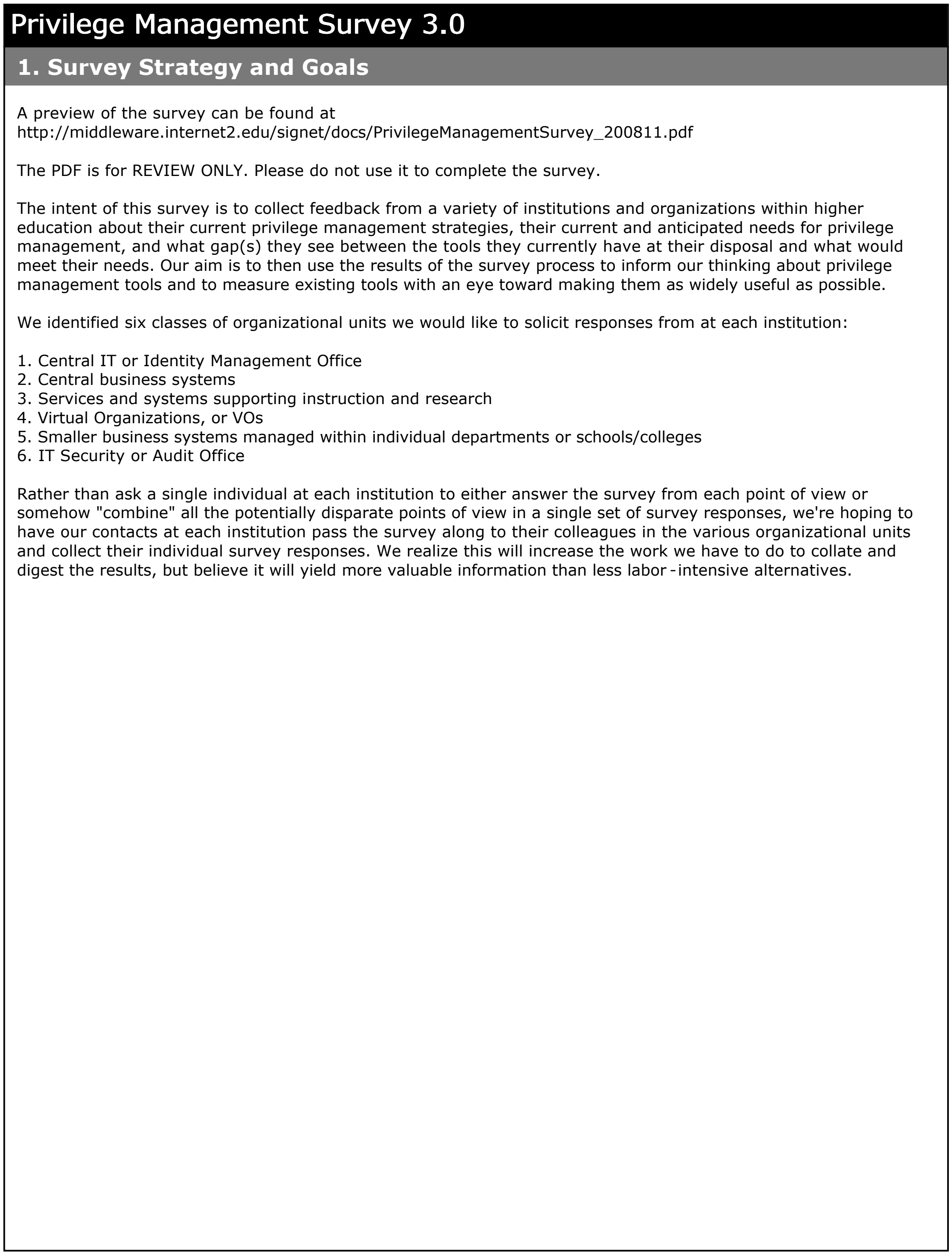
- 100% of sites rank APIs as highly important
- Roles > Groups > Affiliations
- Everybody loves rules; not people
- Current state reporting > Historical auditing
- Attestation, temporary privilege transfer are divisive



Next Steps

- Solicit responses from EDUCAUSE IdM
- Component analysis
  - Public vs. Private?
  - Large vs. Small? R-1, etc.?
- Functional & Technical implementation recommendations

Appendix B: Survey Questions



Privilege Management Survey 3.0

1. Survey Strategy and Goals

A preview of the survey can be found at
http://middleware.internet2.edu/signet/docs/PrivilegeManagementSurvey_200811.pdf

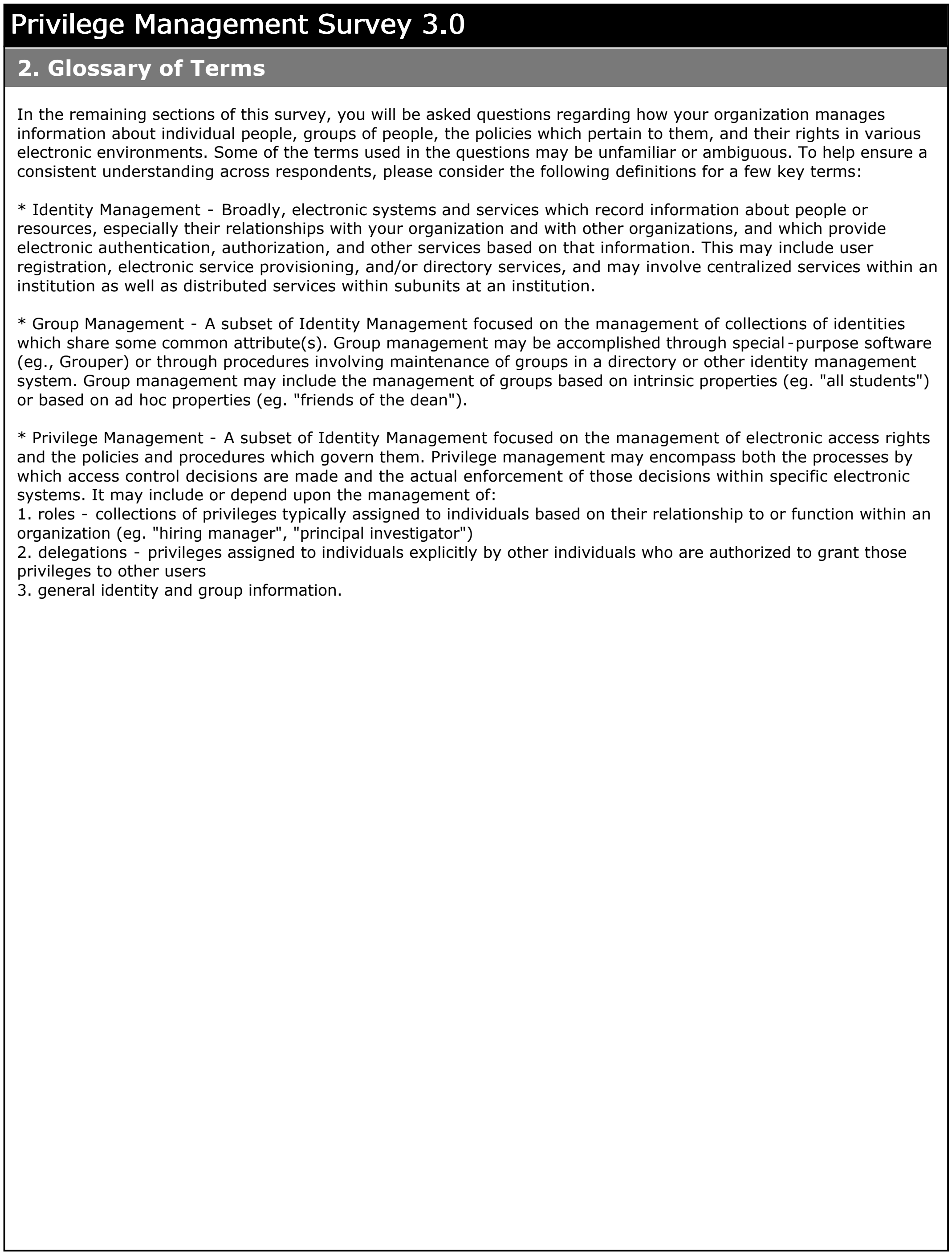
The PDF is for REVIEW ONLY. Please do not use it to complete the survey.

The intent of this survey is to collect feedback from a variety of institutions and organizations within higher education about their current privilege management strategies, their current and anticipated needs for privilege management, and what gap(s) they see between the tools they currently have at their disposal and what would meet their needs. Our aim is to then use the results of the survey process to inform our thinking about privilege management tools and to measure existing tools with an eye toward making them as widely useful as possible.

We identified six classes of organizational units we would like to solicit responses from at each institution:

1. Central IT or Identity Management Office
2. Central business systems
3. Services and systems supporting instruction and research
4. Virtual Organizations, or VOs
5. Smaller business systems managed within individual departments or schools/colleges
6. IT Security or Audit Office

Rather than ask a single individual at each institution to either answer the survey from each point of view or somehow "combine" all the potentially disparate points of view in a single set of survey responses, we're hoping to have our contacts at each institution pass the survey along to their colleagues in the various organizational units and collect their individual survey responses. We realize this will increase the work we have to do to collate and digest the results, but believe it will yield more valuable information than less labor-intensive alternatives.



Privilege Management Survey 3.0

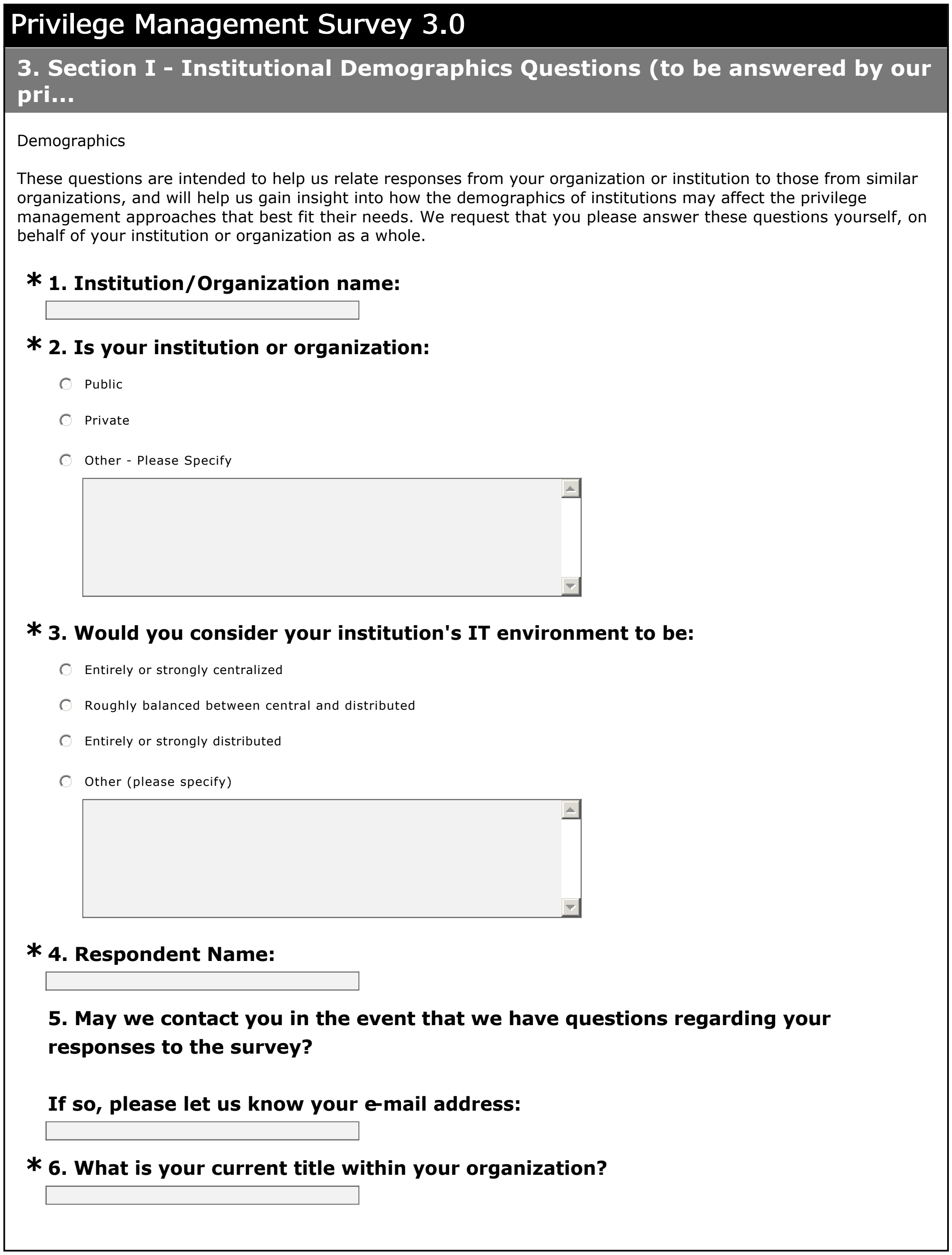
2. Glossary of Terms

In the remaining sections of this survey, you will be asked questions regarding how your organization manages information about individual people, groups of people, the policies which pertain to them, and their rights in various electronic environments. Some of the terms used in the questions may be unfamiliar or ambiguous. To help ensure a consistent understanding across respondents, please consider the following definitions for a few key terms:

* Identity Management - Broadly, electronic systems and services which record information about people or resources, especially their relationships with your organization and with other organizations, and which provide electronic authentication, authorization, and other services based on that information. This may include user registration, electronic service provisioning, and/or directory services, and may involve centralized services within an institution as well as distributed services within subunits at an institution.

* Group Management - A subset of Identity Management focused on the management of collections of identities which share some common attribute(s). Group management may be accomplished through special-purpose software (eg., Grouper) or through procedures involving maintenance of groups in a directory or other identity management system. Group management may include the management of groups based on intrinsic properties (eg. "all students") or based on ad hoc properties (eg. "friends of the dean").

* Privilege Management - A subset of Identity Management focused on the management of electronic access rights and the policies and procedures which govern them. Privilege management may encompass both the processes by which access control decisions are made and the actual enforcement of those decisions within specific electronic systems. It may include or depend upon the management of:
1. roles - collections of privileges typically assigned to individuals based on their relationship to or function within an organization (eg. "hiring manager", "principal investigator")
2. delegations - privileges assigned to individuals explicitly by other individuals who are authorized to grant those privileges to other users
3. general identity and group information.



Privilege Management Survey 3.0

3. Section I - Institutional Demographics Questions (to be answered by our pri...

Demographics

These questions are intended to help us relate responses from your organization or institution to those from similar organizations, and will help us gain insight into how the demographics of institutions may affect the privilege management approaches that best fit their needs. We request that you please answer these questions yourself, on behalf of your institution or organization as a whole.

*** 1. Institution/Organization name:**

*** 2. Is your institution or organization:**

○ Public

○ Private

○ Other - Please Specify

*** 3. Would you consider your institution's IT environment to be:**

○ Entirely or strongly centralized

○ Roughly balanced between central and distributed

○ Entirely or strongly distributed

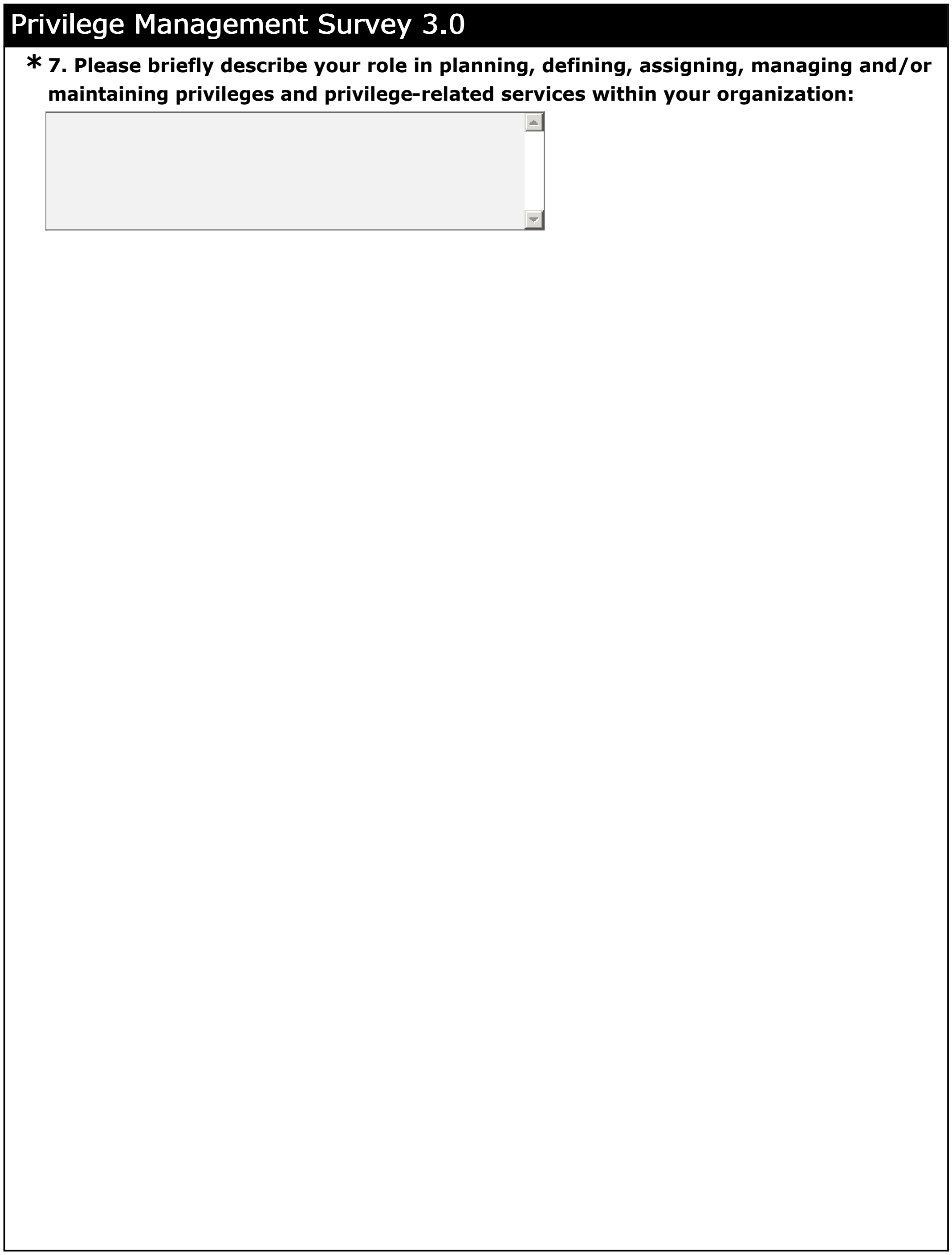
○ Other (please specify)

*** 4. Respondent Name:**

5. May we contact you in the event that we have questions regarding your responses to the survey?

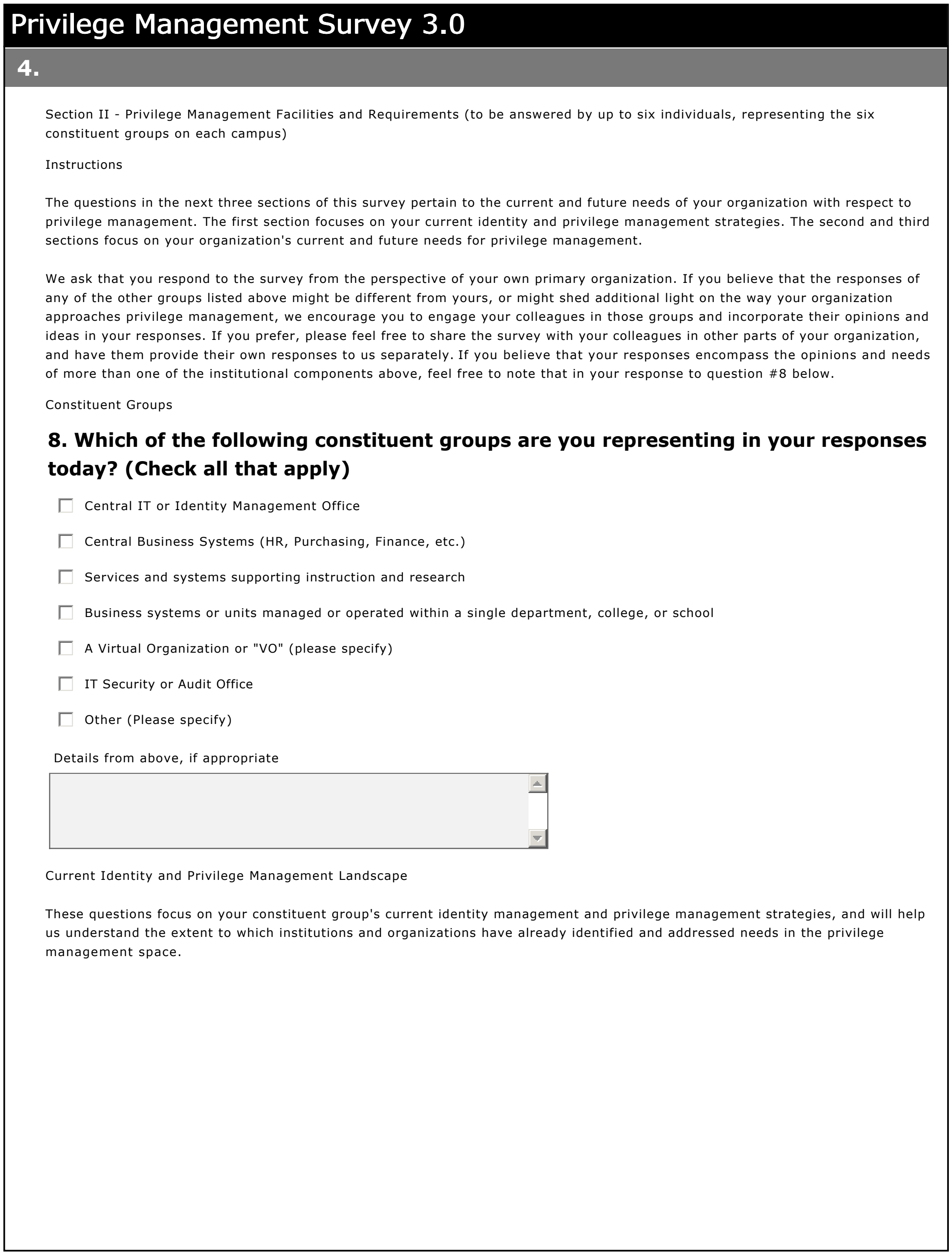
If so, please let us know your e-mail address:

*** 6. What is your current title within your organization?**



Privilege Management Survey 3.0

* **7. Please briefly describe your role in planning, defining, assigning, managing and/or maintaining privileges and privilege-related services within your organization:**



Privilege Management Survey 3.0

4.

Section II - Privilege Management Facilities and Requirements (to be answered by up to six individuals, representing the six constituent groups on each campus)

Instructions

The questions in the next three sections of this survey pertain to the current and future needs of your organization with respect to privilege management. The first section focuses on your current identity and privilege management strategies. The second and third sections focus on your organization's current and future needs for privilege management.

We ask that you respond to the survey from the perspective of your own primary organization. If you believe that the responses of any of the other groups listed above might be different from yours, or might shed additional light on the way your organization approaches privilege management, we encourage you to engage your colleagues in those groups and incorporate their opinions and ideas in your responses. If you prefer, please feel free to share the survey with your colleagues in other parts of your organization, and have them provide their own responses to us separately. If you believe that your responses encompass the opinions and needs of more than one of the institutional components above, feel free to note that in your response to question #8 below.

Constituent Groups

8. Which of the following constituent groups are you representing in your responses today? (Check all that apply)

□ Central IT or Identity Management Office

□ Central Business Systems (HR, Purchasing, Finance, etc.)

□ Services and systems supporting instruction and research

□ Business systems or units managed or operated within a single department, college, or school

□ A Virtual Organization or "VO" (please specify)

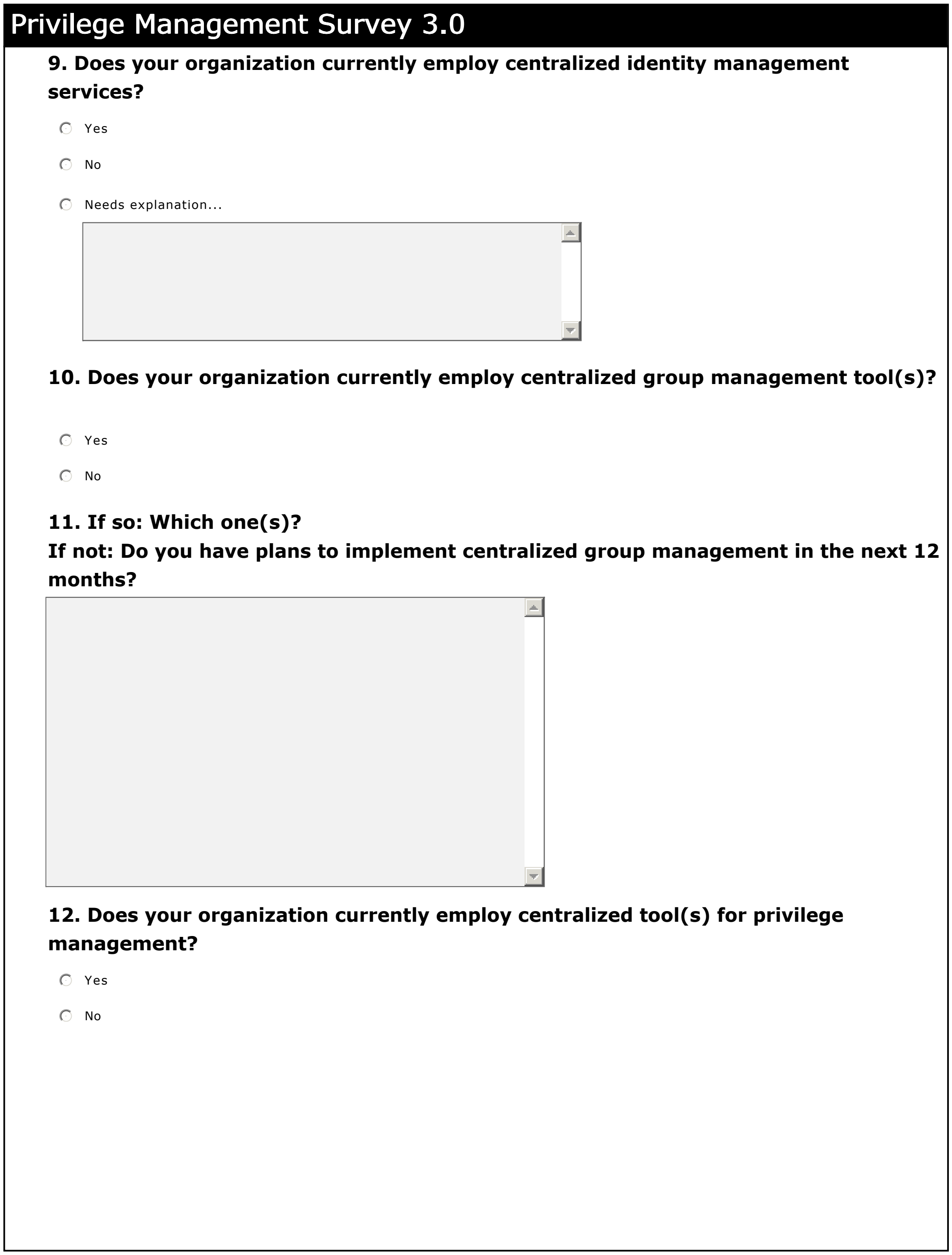
□ IT Security or Audit Office

□ Other (Please specify)

Details from above, if appropriate

Current Identity and Privilege Management Landscape

These questions focus on your constituent group's current identity management and privilege management strategies, and will help us understand the extent to which institutions and organizations have already identified and addressed needs in the privilege management space.



Privilege Management Survey 3.0

9. Does your organization currently employ centralized identity management services?

○ Yes

○ No

○ Needs explanation...

10. Does your organization currently employ centralized group management tool(s)?

○ Yes

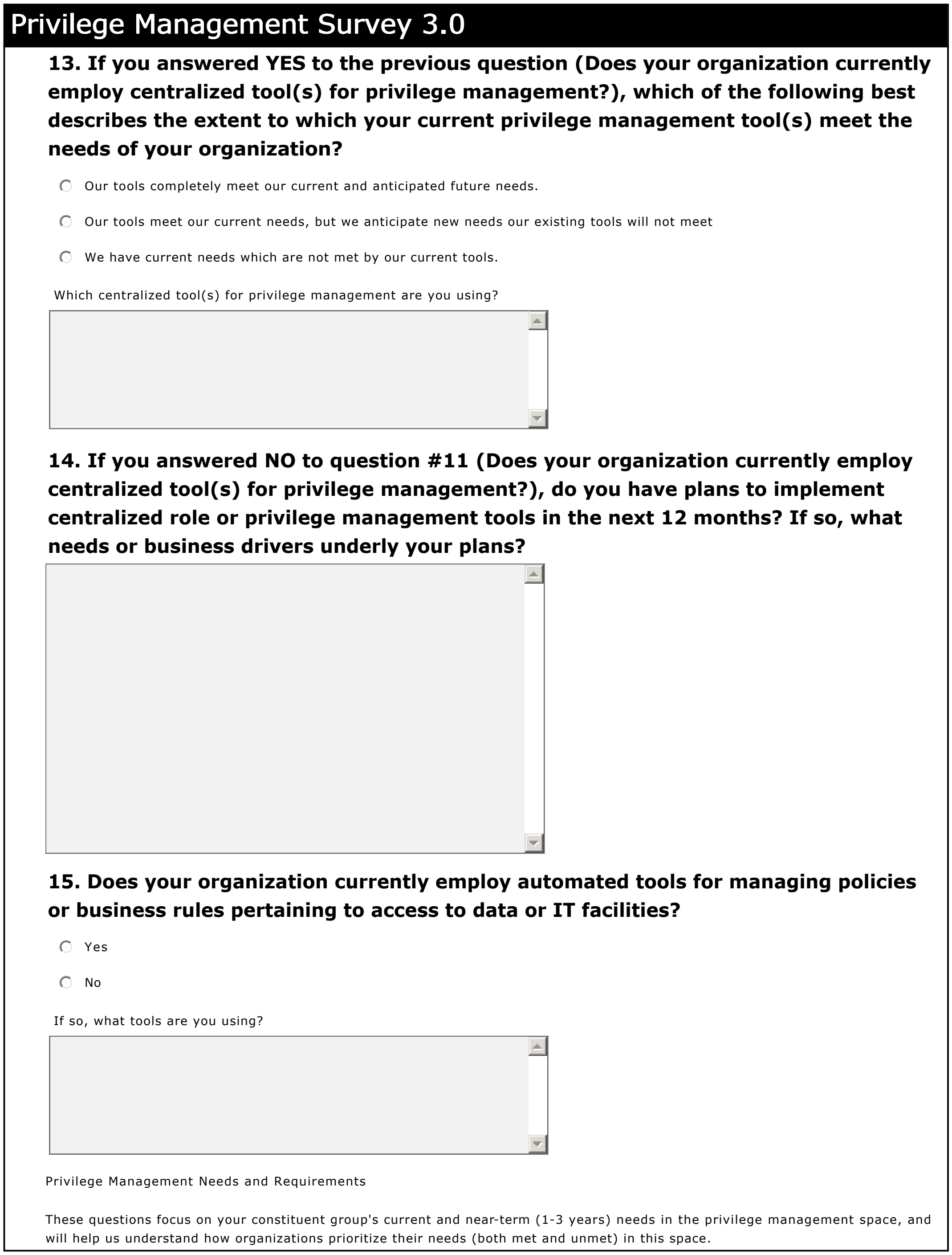
○ No

11. If so: Which one(s)?
If not: Do you have plans to implement centralized group management in the next 12 months?

12. Does your organization currently employ centralized tool(s) for privilege management?

○ Yes

○ No



Privilege Management Survey 3.0

13. If you answered YES to the previous question (Does your organization currently employ centralized tool(s) for privilege management?), which of the following best describes the extent to which your current privilege management tool(s) meet the needs of your organization?

○ Our tools completely meet our current and anticipated future needs.

○ Our tools meet our current needs, but we anticipate new needs our existing tools will not meet

○ We have current needs which are not met by our current tools.

Which centralized tool(s) for privilege management are you using?

14. If you answered NO to question #11 (Does your organization currently employ centralized tool(s) for privilege management?), do you have plans to implement centralized role or privilege management tools in the next 12 months? If so, what needs or business drivers underly your plans?

15. Does your organization currently employ automated tools for managing policies or business rules pertaining to access to data or IT facilities?

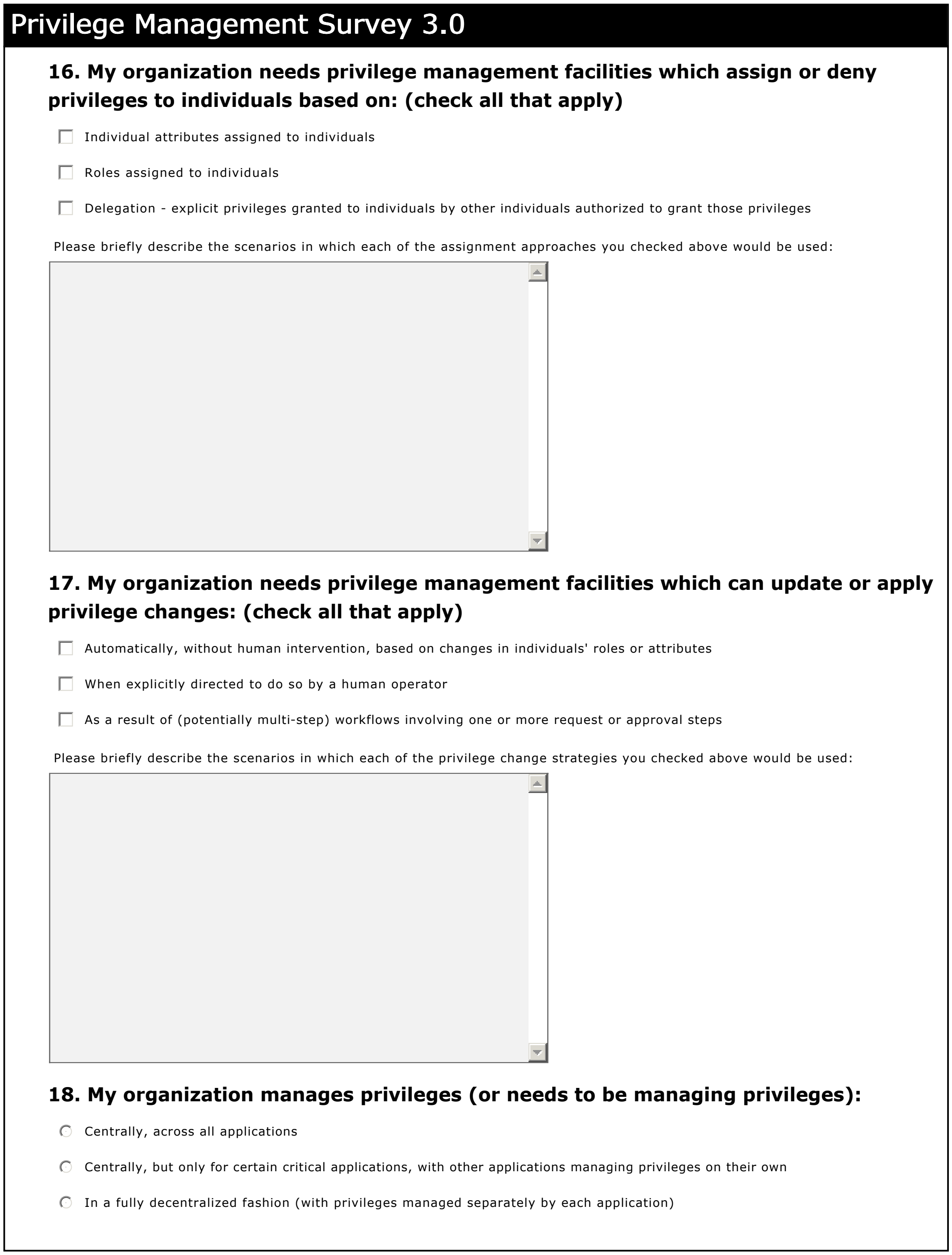
○ Yes

○ No

If so, what tools are you using?

Privilege Management Needs and Requirements

These questions focus on your constituent group's current and near-term (1-3 years) needs in the privilege management space, and will help us understand how organizations prioritize their needs (both met and unmet) in this space.



Privilege Management Survey 3.0

16. My organization needs privilege management facilities which assign or deny privileges to individuals based on: (check all that apply)

□ Individual attributes assigned to individuals

□ Roles assigned to individuals

□ Delegation - explicit privileges granted to individuals by other individuals authorized to grant those privileges

Please briefly describe the scenarios in which each of the assignment approaches you checked above would be used:

17. My organization needs privilege management facilities which can update or apply privilege changes: (check all that apply)

□ Automatically, without human intervention, based on changes in individuals' roles or attributes

□ When explicitly directed to do so by a human operator

□ As a result of (potentially multi-step) workflows involving one or more request or approval steps

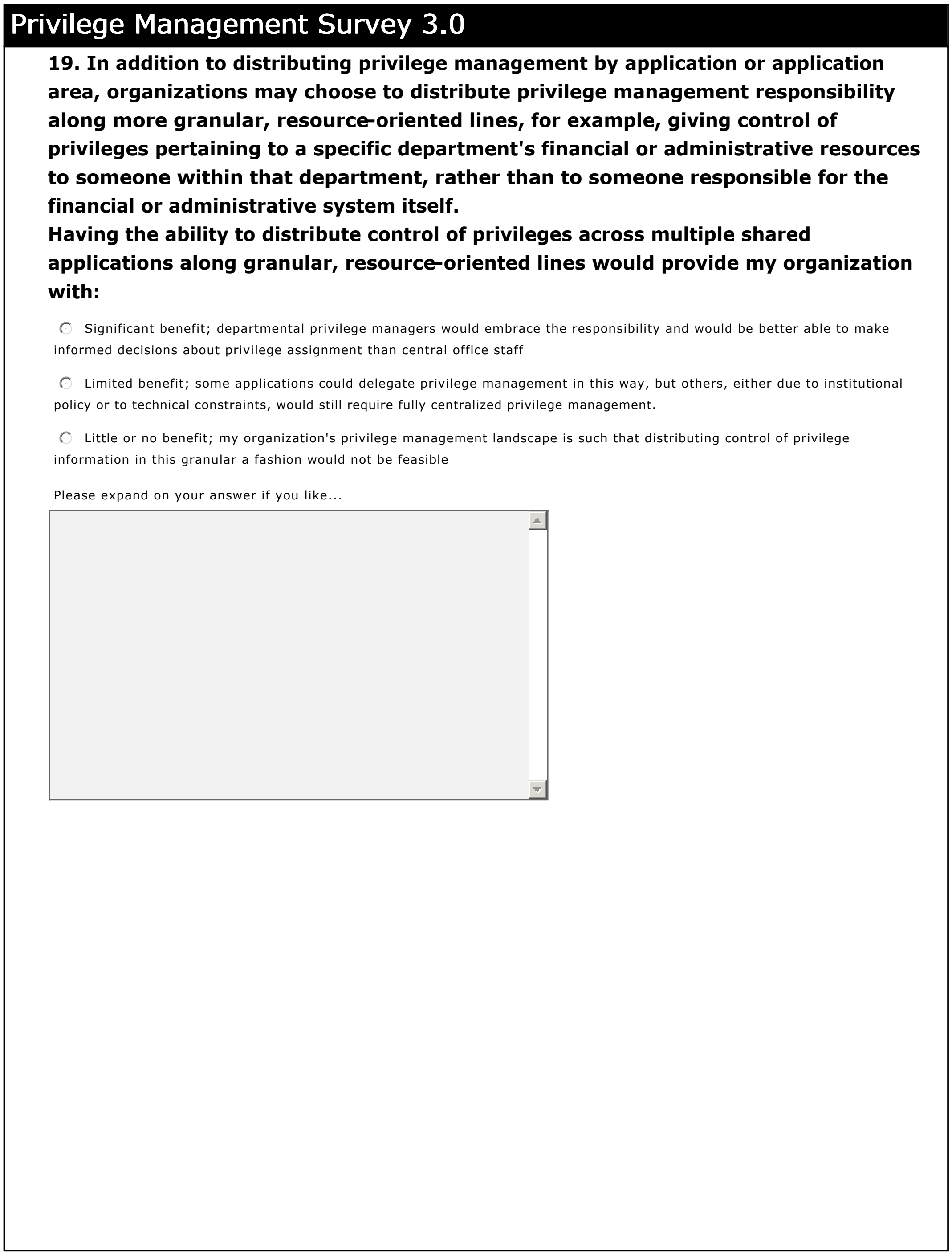
Please briefly describe the scenarios in which each of the privilege change strategies you checked above would be used:

18. My organization manages privileges (or needs to be managing privileges):

○ Centrally, across all applications

○ Centrally, but only for certain critical applications, with other applications managing privileges on their own

○ In a fully decentralized fashion (with privileges managed separately by each application)



Privilege Management Survey 3.0

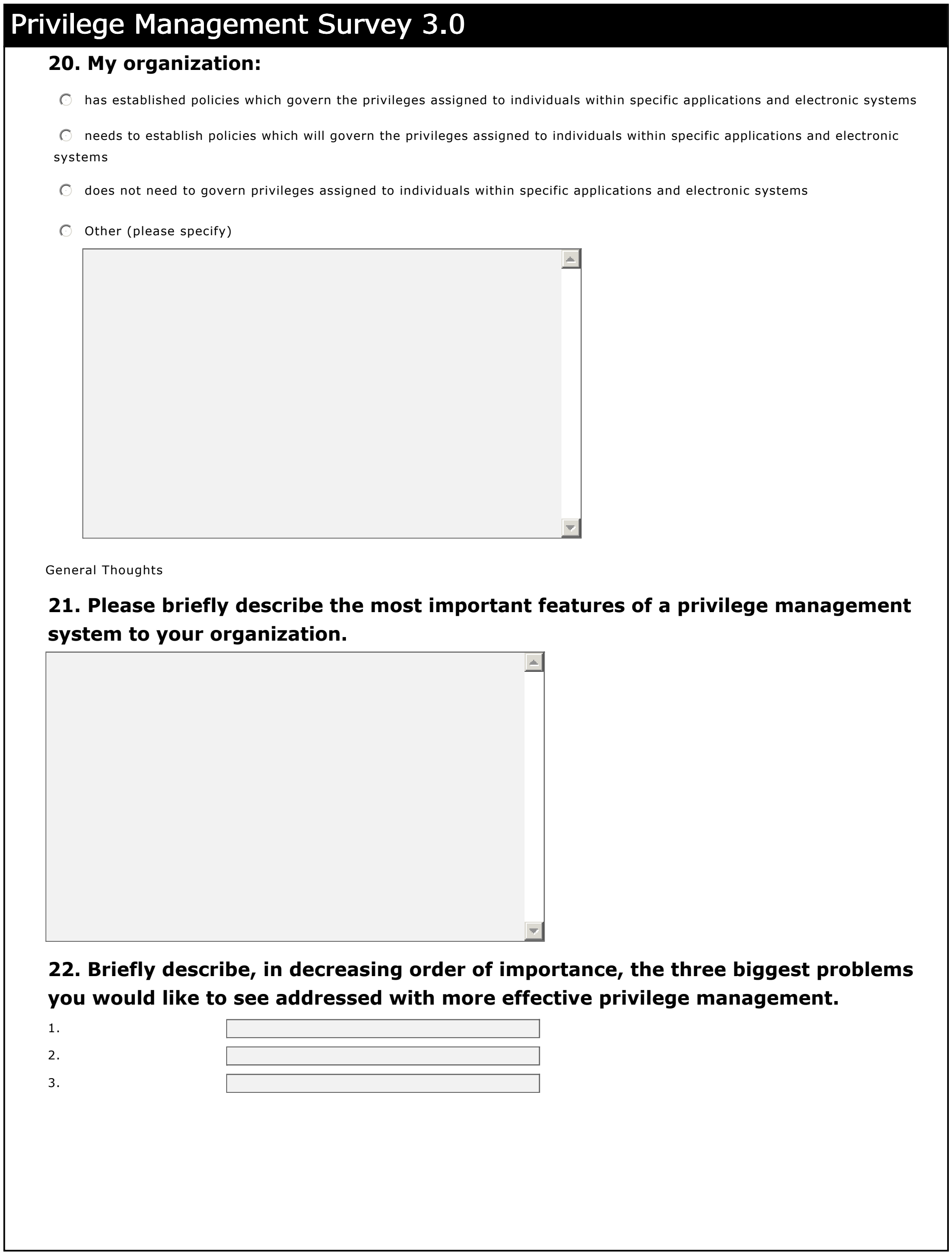
19. In addition to distributing privilege management by application or application area, organizations may choose to distribute privilege management responsibility along more granular, resource-oriented lines, for example, giving control of privileges pertaining to a specific department's financial or administrative resources to someone within that department, rather than to someone responsible for the financial or administrative system itself.
Having the ability to distribute control of privileges across multiple shared applications along granular, resource-oriented lines would provide my organization with:

○ Significant benefit; departmental privilege managers would embrace the responsibility and would be better able to make informed decisions about privilege assignment than central office staff

○ Limited benefit; some applications could delegate privilege management in this way, but others, either due to institutional policy or to technical constraints, would still require fully centralized privilege management.

○ Little or no benefit; my organization's privilege management landscape is such that distributing control of privilege information in this granular a fashion would not be feasible

Please expand on your answer if you like...



Privilege Management Survey 3.0

20. My organization:

○ has established policies which govern the privileges assigned to individuals within specific applications and electronic systems

○ needs to establish policies which will govern the privileges assigned to individuals within specific applications and electronic systems

○ does not need to govern privileges assigned to individuals within specific applications and electronic systems

○ Other (please specify)

General Thoughts

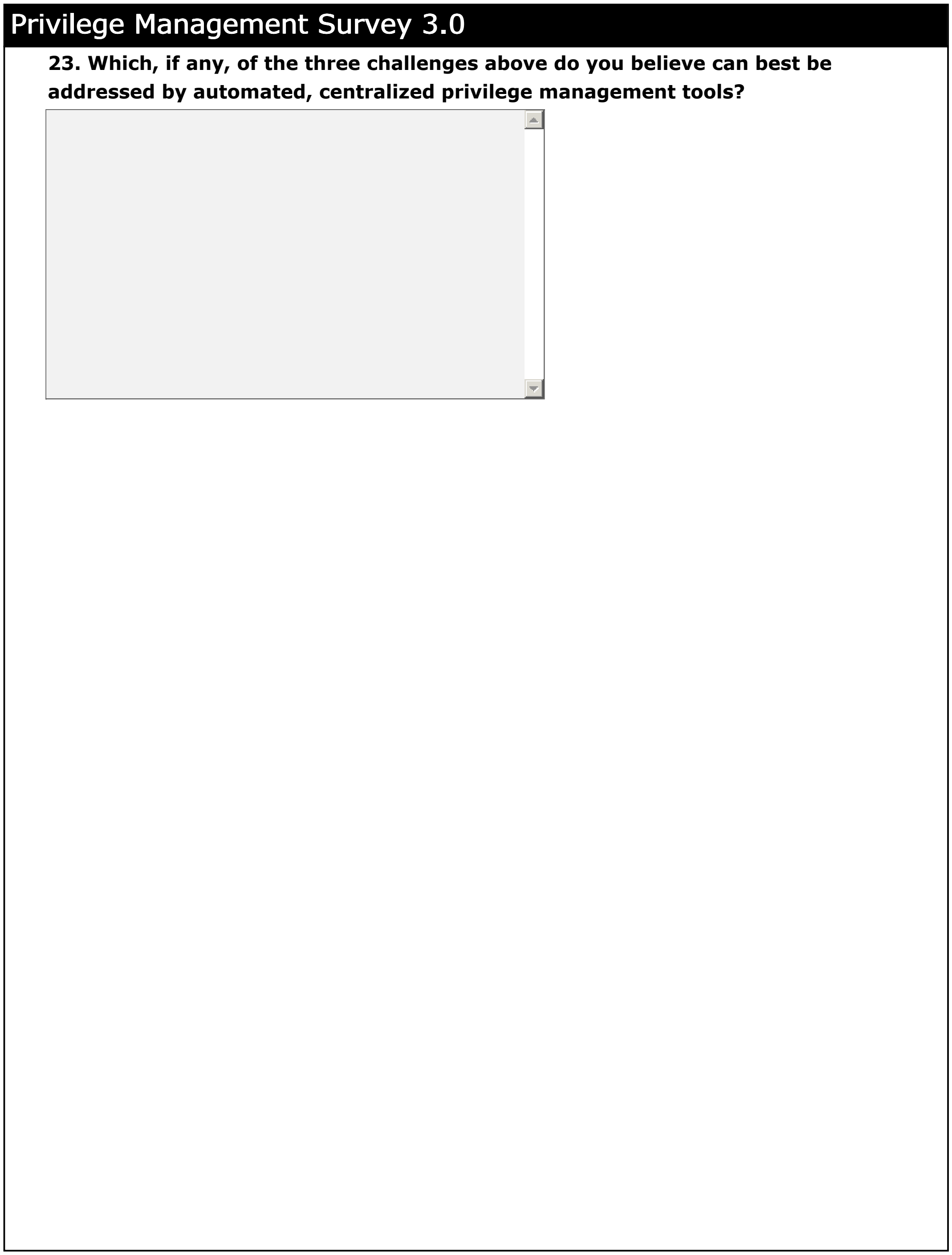
21. Please briefly describe the most important features of a privilege management system to your organization.

22. Briefly describe, in decreasing order of importance, the three biggest problems you would like to see addressed with more effective privilege management.

1.

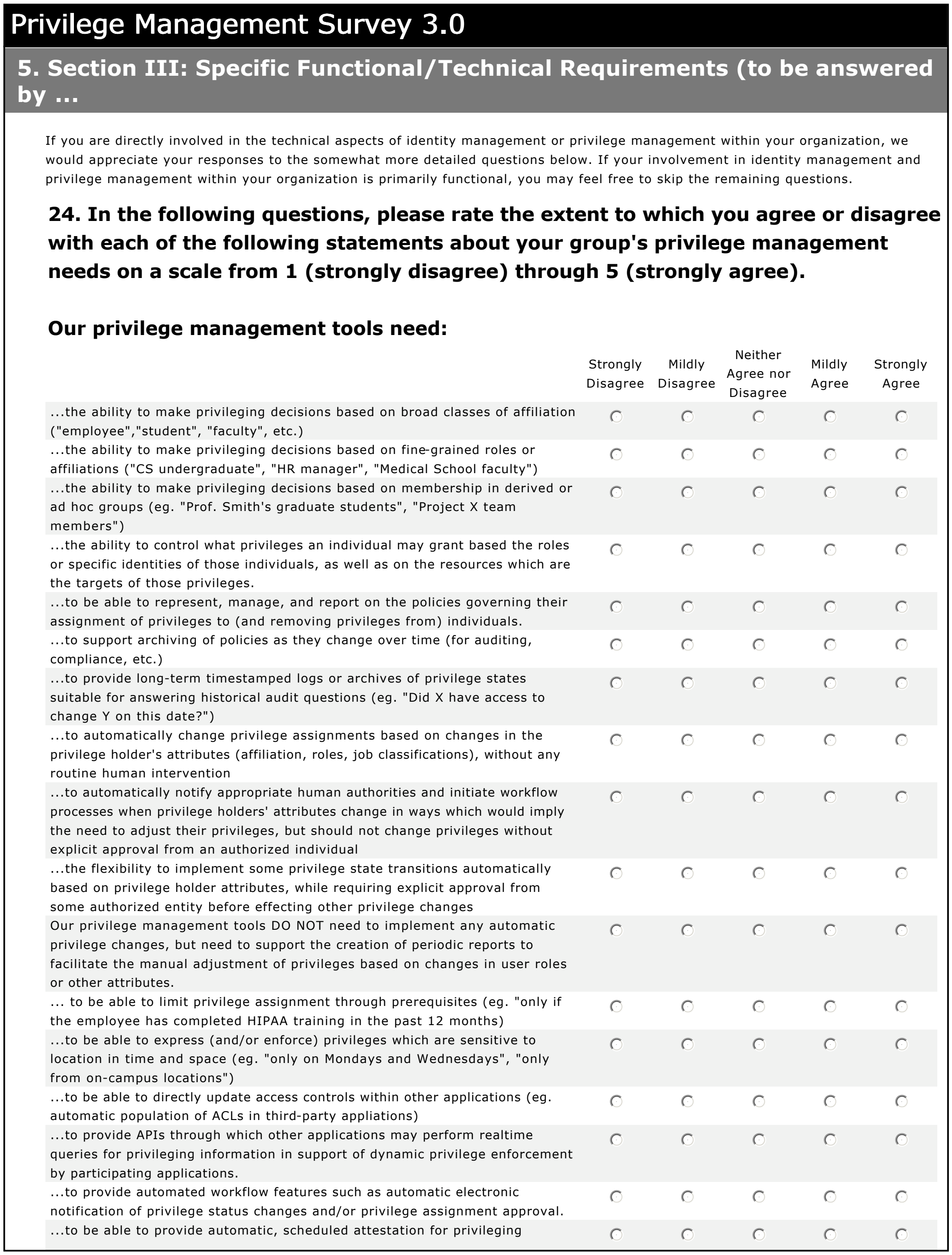
2.

3.



Privilege Management Survey 3.0

23. Which, if any, of the three challenges above do you believe can best be addressed by automated, centralized privilege management tools?



Privilege Management Survey 3.0

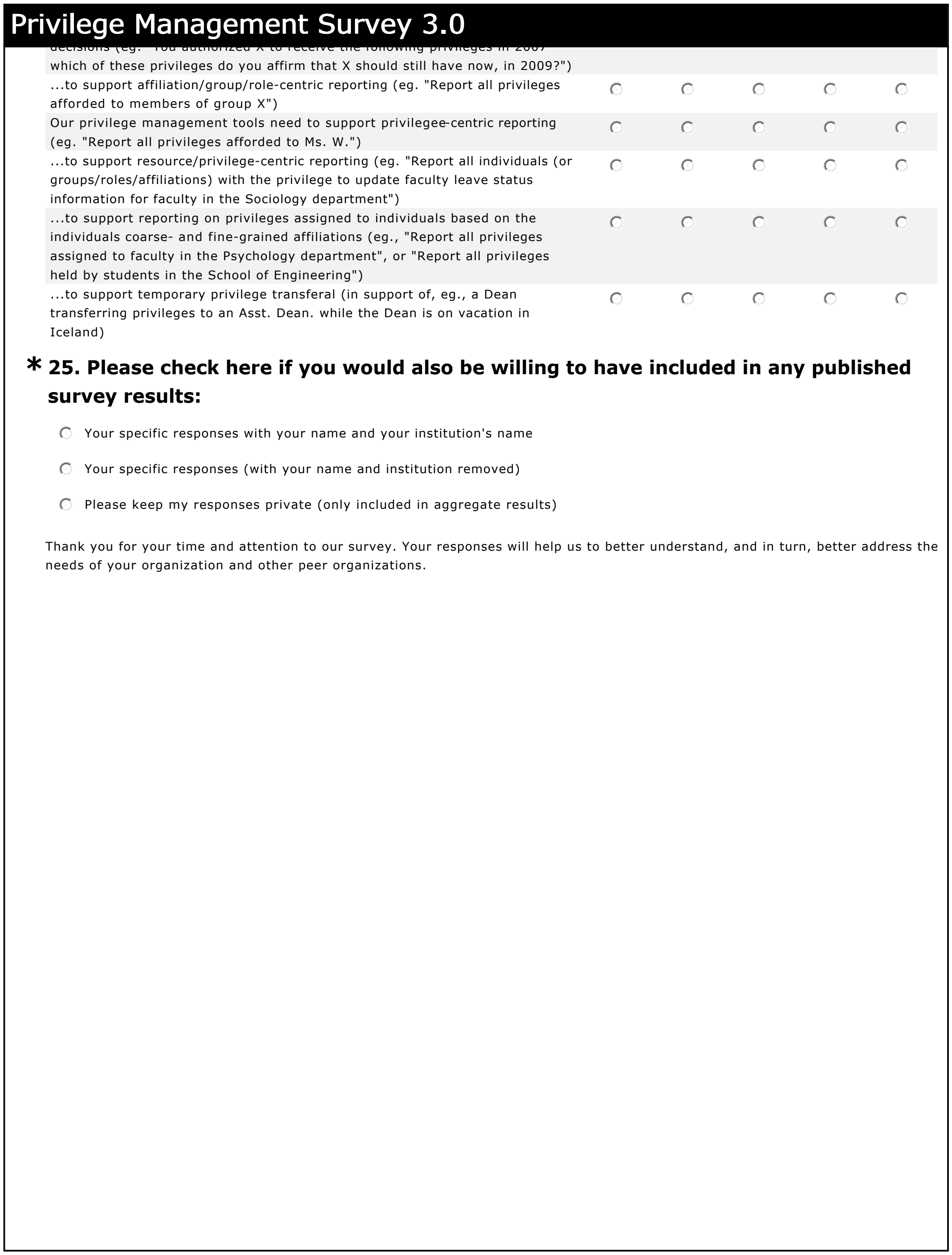
5. Section III: Specific Functional/Technical Requirements (to be answered by ...

If you are directly involved in the technical aspects of identity management or privilege management within your organization, we would appreciate your responses to the somewhat more detailed questions below. If your involvement in identity management and privilege management within your organization is primarily functional, you may feel free to skip the remaining questions.

24. In the following questions, please rate the extent to which you agree or disagree with each of the following statements about your group's privilege management needs on a scale from 1 (strongly disagree) through 5 (strongly agree).

Our privilege management tools need:

	Strongly Disagree	Mildly Disagree	Neither Agree nor Disagree	Mildly Agree	Strongly Agree
...the ability to make privileging decisions based on broad classes of affiliation ("employee","student", "faculty", etc.)	○	○	○	○	○
...the ability to make privileging decisions based on fine-grained roles or affiliations ("CS undergraduate", "HR manager", "Medical School faculty")	○	○	○	○	○
...the ability to make privileging decisions based on membership in derived or ad hoc groups (eg. "Prof. Smith's graduate students", "Project X team members")	○	○	○	○	○
...the ability to control what privileges an individual may grant based the roles or specific identities of those individuals, as well as on the resources which are the targets of those privileges.	○	○	○	○	○
...to be able to represent, manage, and report on the policies governing their assignment of privileges to (and removing privileges from) individuals.	○	○	○	○	○
...to support archiving of policies as they change over time (for auditing, compliance, etc.)	○	○	○	○	○
...to provide long-term timestamped logs or archives of privilege states suitable for answering historical audit questions (eg. "Did X have access to change Y on this date?")	○	○	○	○	○
...to automatically change privilege assignments based on changes in the privilege holder's attributes (affiliation, roles, job classifications), without any routine human intervention	○	○	○	○	○
...to automatically notify appropriate human authorities and initiate workflow processes when privilege holders' attributes change in ways which would imply the need to adjust their privileges, but should not change privileges without explicit approval from an authorized individual	○	○	○	○	○
...the flexibility to implement some privilege state transitions automatically based on privilege holder attributes, while requiring explicit approval from some authorized entity before effecting other privilege changes	○	○	○	○	○
Our privilege management tools DO NOT need to implement any automatic privilege changes, but need to support the creation of periodic reports to facilitate the manual adjustment of privileges based on changes in user roles or other attributes.	○	○	○	○	○
... to be able to limit privilege assignment through prerequisites (eg. "only if the employee has completed HIPAA training in the past 12 months)	○	○	○	○	○
...to be able to express (and/or enforce) privileges which are sensitive to location in time and space (eg. "only on Mondays and Wednesdays", "only from on-campus locations")	○	○	○	○	○
...to be able to directly update access controls within other applications (eg. automatic population of ACLs in third-party appliations)	○	○	○	○	○
...to provide APIs through which other applications may perform realtime queries for privileging information in support of dynamic privilege enforcement by participating applications.	○	○	○	○	○
...to provide automated workflow features such as automatic electronic notification of privilege status changes and/or privilege assignment approval.	○	○	○	○	○
...to be able to provide automatic, scheduled attestation for privileging	○	○	○	○	○



Privilege Management Survey 3.0

decisions (eg. "You authorized X to receive the following privileges in 2007 which of these privileges do you affirm that X should still have now, in 2009?")					
...to support affiliation/group/role-centric reporting (eg. "Report all privileges afforded to members of group X")	○	○	○	○	○
Our privilege management tools need to support privilegee-centric reporting (eg. "Report all privileges afforded to Ms. W.")	○	○	○	○	○
...to support resource/privilege-centric reporting (eg. "Report all individuals (or groups/roles/affiliations) with the privilege to update faculty leave status information for faculty in the Sociology department")	○	○	○	○	○
...to support reporting on privileges assigned to individuals based on the individuals coarse- and fine-grained affiliations (eg., "Report all privileges assigned to faculty in the Psychology department", or "Report all privileges held by students in the School of Engineering")	○	○	○	○	○
...to support temporary privilege transferal (in support of, eg., a Dean transferring privileges to an Asst. Dean. while the Dean is on vacation in Iceland)	○	○	○	○	○

*** 25. Please check here if you would also be willing to have included in any published survey results:**

○ Your specific responses with your name and your institution's name

○ Your specific responses (with your name and institution removed)

○ Please keep my responses private (only included in aggregate results)

Thank you for your time and attention to our survey. Your responses will help us to better understand, and in turn, better address the needs of your organization and other peer organizations.