Access Review Survey Report

Please note that this is the draft version of the report. Some sections might be unfinished or incomplete.

April 12, 2014

1 Introduction

Our interviews shed light on how access review are performed in the organizations, and what are the challenges faced by security practitioners and managers in access review activity. The findings of the field study helped us formulate access review as a human activity, and observe the importance of helping certifiers make decisions more accurately and efficiently. One the other hand, the details of how access review was performed differed between participants. For example, some of our participants said managers are responsible for review of their employees, and some of our participants said application owners are responsible for review. Some companies used roles, and reviewed roles during access review, some companies used permissions and reviewed those. To further understand the state of the practice in access review, and collect quantitative results on how companies perform access review, we conducted a survey of security practitioners.

2 Survey Goal and Methodology

We designed the survey with three goals in mind: (1) Clarify certain findings in the interview study, in which we observed contrasting results. (2) Collect quantitative data that can help us in designing a new interface for access review. (3) Collect data that help us design an ecologically valid study to test the AuthzMap interface.

In particular we tried to answer the following questions:

1. what determines the access of a user to an application? coarse grain application access, roles, or entitlements?
2. who is responsible for performing access certification in organizations?
3. is there a relationship between the organizational context and the way access certification is performed?

4. what stakeholders are involved in access certification, and how they collaborate with each other?

5. what information can be used to help access certification?

6. what is an indication of risk when evaluating access rights of users?

Answering questions 1-3 help us design a technology that can work in the organizational context in which access certification is performed, and answering questions 3-6, help us design a technology that improves the accuracy and efficiency of access certification.

To answer the aforementioned research questions, we designed a questionnaire with 20 questions. The questions were a combination of closed and open-ended questions, and participants were allowed to skip answering any of them. Based on our previous experience, the target audience for the survey are security practitioners who are busy, and not willing to spend long period of time on a study.

Therefore, we tried to minimize the time required for completing the survey (between 10 and 15 minutes). The survey had the following components:

introduction and consent: at the beginning of the survey, we presented the participants with the purpose of the survey, and a consent form. Upon participants' consent, we show them the questions.

demographics: we collected demographics information about the participants, including their job title, years of experience in IT security and IdM, and their experience with various IdM systems.

organizational context: we collected information about the organizational size, sector, and location, the level of IdM adoption in the organization, wether the organization adopted roles for managing access, and the legislative requirements that the organization needs to comply with.

state of access certification in the organization: we collected data on the process of access certification, who performs it, frequency of certification, and what triggers certification.

access certification preferences: in the last section of the survey, we asked participants to determine their preference for communication channels during certification, the information items that might be useful during the certification, and the risk associated with different observation during access certification. This data will help us designing a better technological solution for access certification.

closing page: we thanked the participants for their participation, and provide them with an option to enter their name and email address, if they liked to be contacted for a follow-up study.

3 Recruitement

We distributed the survey through Linked-In communities. The link and description of the survey was posted twice to three different Linked-In groups with the focus on identity and access management (the three groups had 12125, 8792, 4598 members at the time of conducting the survey). Also the link to the survey were posted on forums related to identity and access management, including support forums for CA, Oracle, and Novel identity management systems. We also posted the link to the survey to the Forrester Research discussion forum. Unfortunately, these recruitment efforts did not lead to recruitement of any participants. But we received a request from Forrester Research company, and they showed interest in collaborating with us in publicizing the survey, in exchange for survey data. As a result, we seek help from Forrester research company. We used their social media channels (including their blog and twitter feed) to distribute the survey notice. To motivate the participants to participants, we promis that they will enter in a raffle for a 128Gb iPad, and they will receive a complementary report of the survey results from Forrester Research. We received 57 responses to the survey, out of which 49 were valid responses (e.g., two participants declined the consent form, and 5 just browsed through the survey).

4 Results

In this section, we summarize the results of the survey.

5 Demographics

We asked about the job title of the respondents in the first question of the survey. Our goal of this question was to determine the stakeholders in organizations that are interested about access review. An overview of participants' response to this question is shown in Figure 1. Our results show that the participants were mostly security consultants and managers. Also the results show that we have very few security administrators responding to the survey. Those participants who chose the other option in survey, have the following job titles: Analyst, Chief Technology Officer (CTO), Business Executive, Director - Financial Controls, Lead IDM Consultant, I&AM Engineering Manager, App support including identity systems, Technical architect IdM & Access management, Software, Developer, Human Factors/Design Research, Solution Architect, System Administration, Sales Rep, Business development IAG, Business Systems Analyst, VP Enterprise Architecture.

We then asked participants about their experience in IT security and experience with identity and access management. The results of these two questions is presented in Figure 3. Our results suggest that there is a strong correlation between

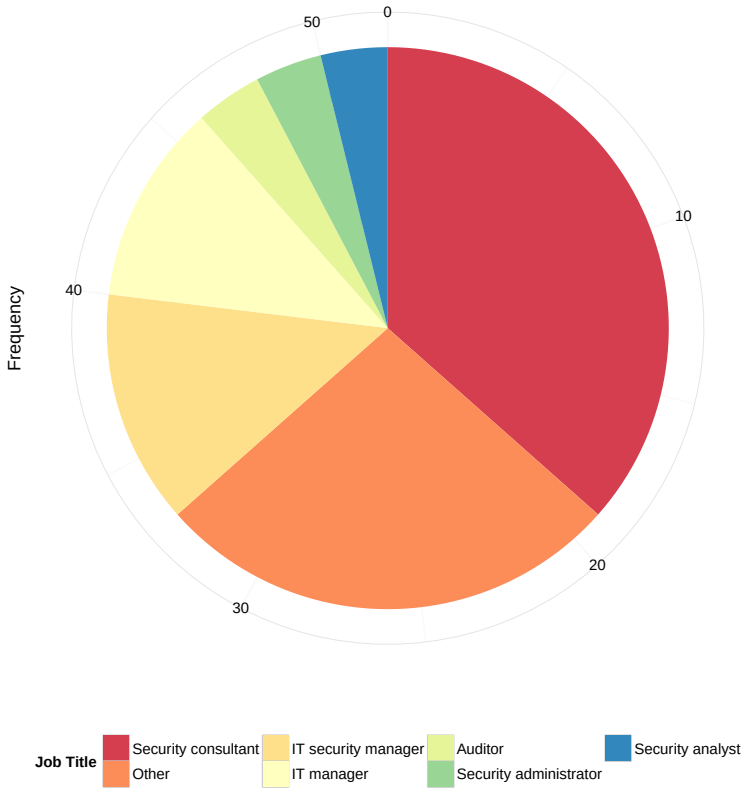


Figure 1: The job function of the participants

the years of IT security experience and IdM experience ($Pearson'sr(47) = 0.70, p < 0.01$). In other words, participants were dealing with AIM problems during their career as a security professional.

6 Organizational Charactristics

We asked participants to identify their organizational sector. Results show that identity and access management is an interest for various organizational sectors. Since we have relatively large number of consultants among the participants, the three main organizational sectors among the top 10 were Business and Computer consulting services, and Systems or Network Integrators. Other notable top 10 sectors were Finance, Banking, Insurance, Medical, and Governmental Agencies. The orgnizational sectors for those participants who chose other were: Analyst, Computer Software, IT (3 participants), Telecom, and Media.

Our participants were from different parts of the world 4. About half of them were from North America, and we had participants from Europe, Asia, and Aus-

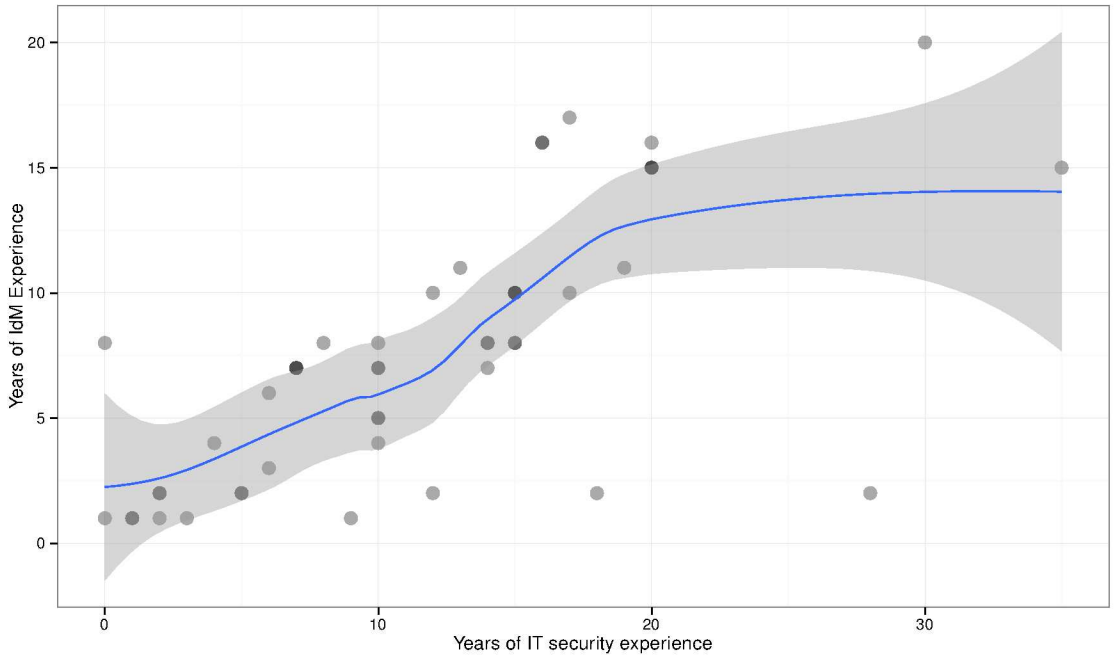


Figure 2: The participants years of IT security and year of identity and access management experience

tralia.

As an indication of the size of company our participants work for, we gave them five options to indicate the number of employees in their respective organization. The results from this question is summarized in Figure 5.

We also asked participants about the security standards that they need to comply with. We listed several standards that we heared about during the interviews, and also give the option of entering other standards that they are complying with to the participants. Participants could select multiple options at the same time for this questions. The participants' responses are summarized in Figure 6. Other than the list of provided standards, participants entered standards such as:

- Personal Information Protection and Electronic Documents Act (PIPEDA) - One instance
- Federal Financial Institutions Examination Council (FFIEC) - Two instances
- NIST SP 800 Series - One instance
- Safe Harbor - One instance
- ITIL (Information Technology Infrastructure Library) security management - One instance

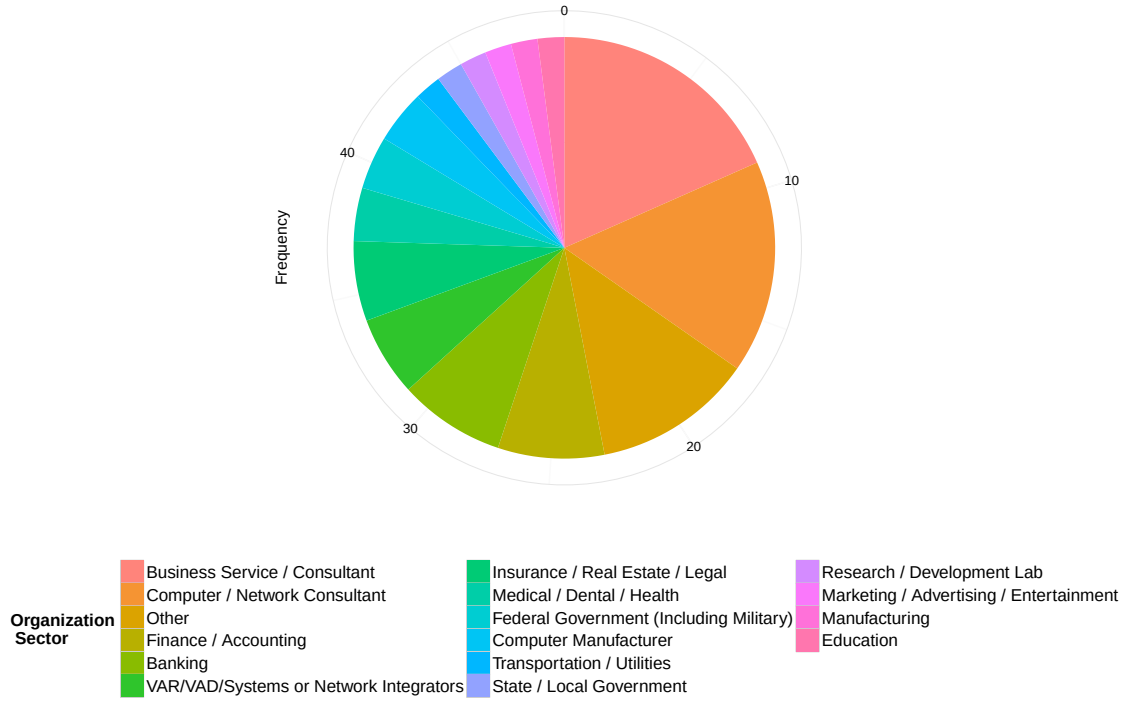


Figure 3: The participants organizational sector

- Critical Security Controls (by SANS Institute) - One instance
- Control Objectives for Information and Related Technology (COBIT) - One instance
- Committee of Sponsoring Organizations (COSO) - One instance

7 State of IdM in Participants Organization

After collecting demographics and organizaional charactristics, we turned our attention to the state of AIM in participants' organization. Our interview study suggested that adopting AIM is a lengthy process, and many organizations only partly adopt an AIM system. Therefore, we asked participants to determine the level of AIM adoption in their company. Indeed the most prevalent answer from the participants were that they partly adopted an AIM system. Also as expected, most of the participants have been in some stage of IdM adoption in their company.

We also investigated the use of role-based access control in the target company. During the interview study we find the implementation of role-based access control as one of the most challenging parts of AIM adoption. Also, some of our par-

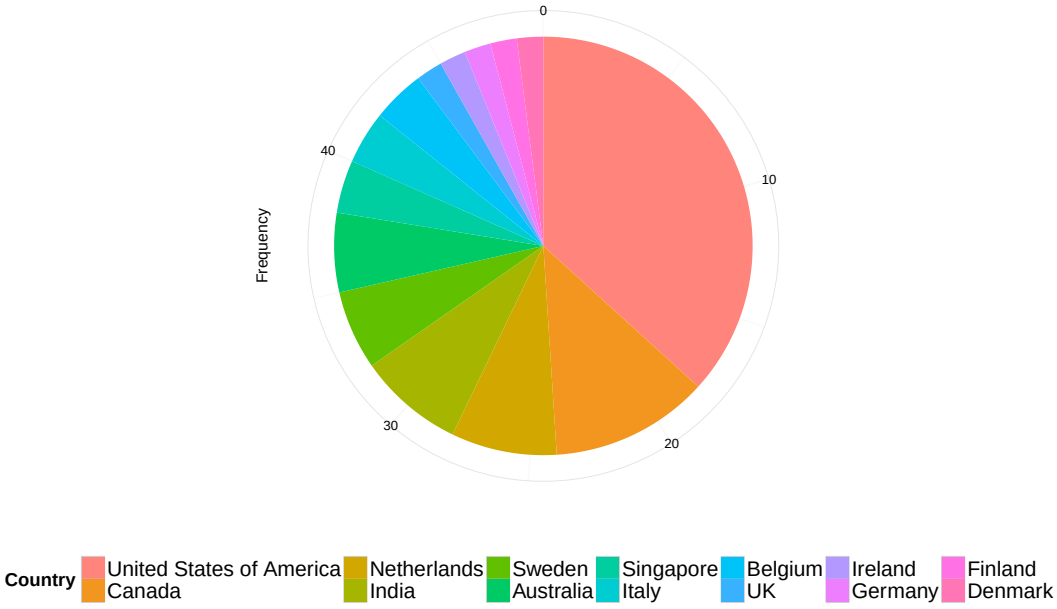


Figure 4: The participants organizational sector

ticipants suggested it is even not viable to completely implement role-based access control. We gave participants the following options: (1) Roles are partly used. Some applications use roles and some use assignment of entitlements to users. (2) Roles are not used, and entitlements are assigned to users to provision them with access. (3) Roles are used throughout the organization, entitlements (access rights) are grouped in roles, and users are assigned to roles to get access to an application. The summary of participants resposes is shown in Figure 8.

8 Details of Access Review Activity

Who performs what: We asked participants about how access review is currently performed in their company, and how it should be performed from their point of view. We received various answers in the interview study, and our goal of this question was to collect quantitative data on how access review should be done, and how far our participants are from their ideal view of access review.

We designed different options based on the field study data, and also added "Other" option to check if the survey participants perform review differently or can think of new approaches. The summary of the responses is shown in Figure 9. For the current state of their company, our provided options were sufficient for the participants, except two. One participant mentioned that they used a mixture of the methods, without providing further details, and one participant mentioned

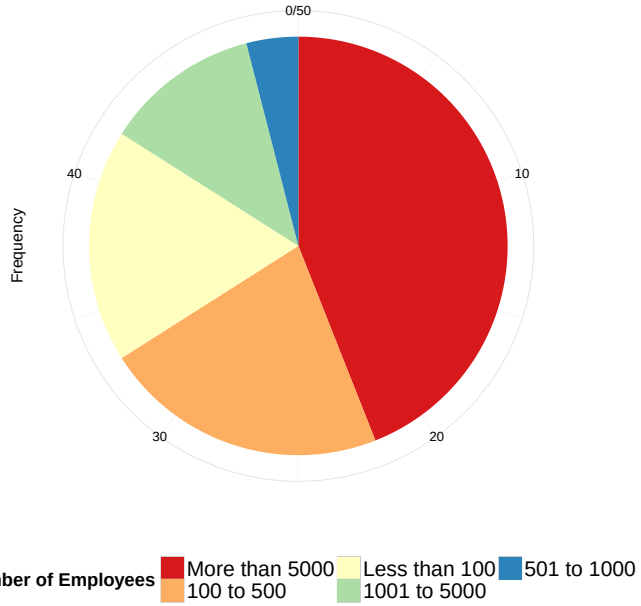


Figure 5: The participants organizational sector

that they review the role structure. For the desired state of access review, participants provided comments beyond provided options in the survey. Some participants suggested different ways of reviewing access in the "Other" field. One participant mentioned that the governance team in the company should review those entitlements that are undecided by the managers. Another participant mentioned that the type of entitlement should determine who reviews it. One participant described that "Role Owners" should also review the access, beside the managers. Furthermore, those people who approved the assignment of user to role should also review the access. One other participant mentioned that while manager and application owner both should review the access, the composition of the roles should be reviewed as well.

How frequent is it: During the interviews we saw that companies perform access review on various frequency levels ranged from once a year to quarterly. Also participants noted that they perform ad-hoc reviews. The goal of this question was to collect data on how frequently companies do access review. Participants could choose multiple answers ranged from Ad-hoc to once a year. The answers to this question is summarized in Figure 10.

Participants also provided comments beyond the provided options in the survey, which mainly clarified ad-hoc reviews. One participant wrote that review should be done *"On Every Employee Job transfer, both by previous and current managers."* Another participant also pointed to the job transfer, and added that review should be done on hiring, and deployment of new applications. Anoter partici-

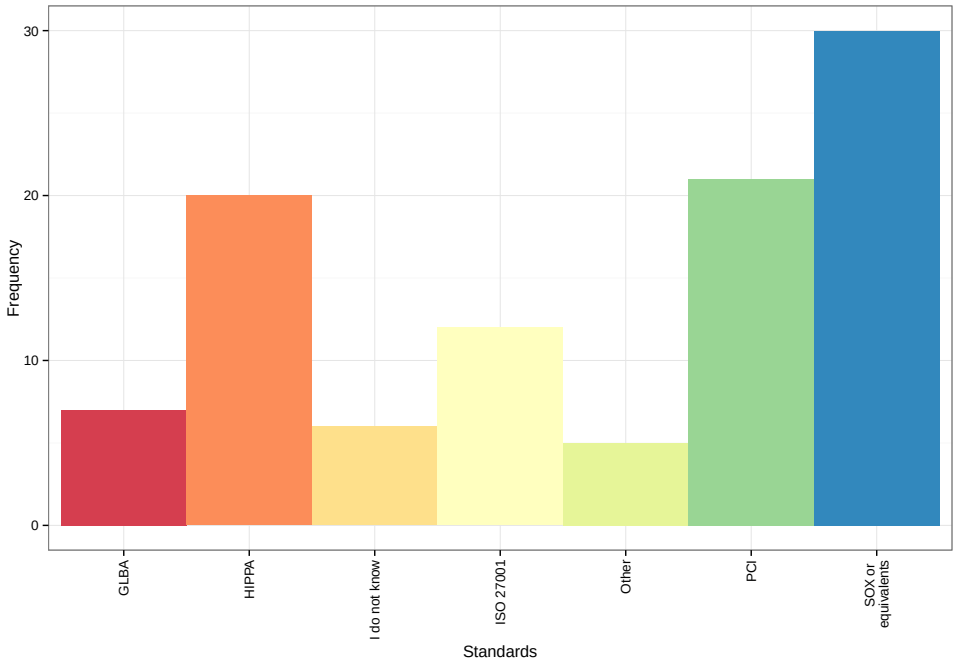


Figure 6: The participants organizational sector

pant mentioned that they determine the review schedule at the beginning of each year, and one other participant said that they do not do it consistently. Finally, one participant said that they do it automatically, and in real-time.

What triggers it: Those participants who talked about ad-hoc access review, also talked about different factors that trigger those ad-hoc reviews. In this question, our goal is to collect quantitative data on what might results in a company performing ad-hoc reviews. We listed the options we saw in our field study data, as well as giving participants to list their own triggers 11:

Participants also provided other triggers for access review such as:

- Change of manager
- Employee separations
- Audit findings
- New projects
- New applications
- Hiring new employees

How access lists are generated: We saw that the main artifact used during access review is the access lists (list of users and their accesses). But we saw that this

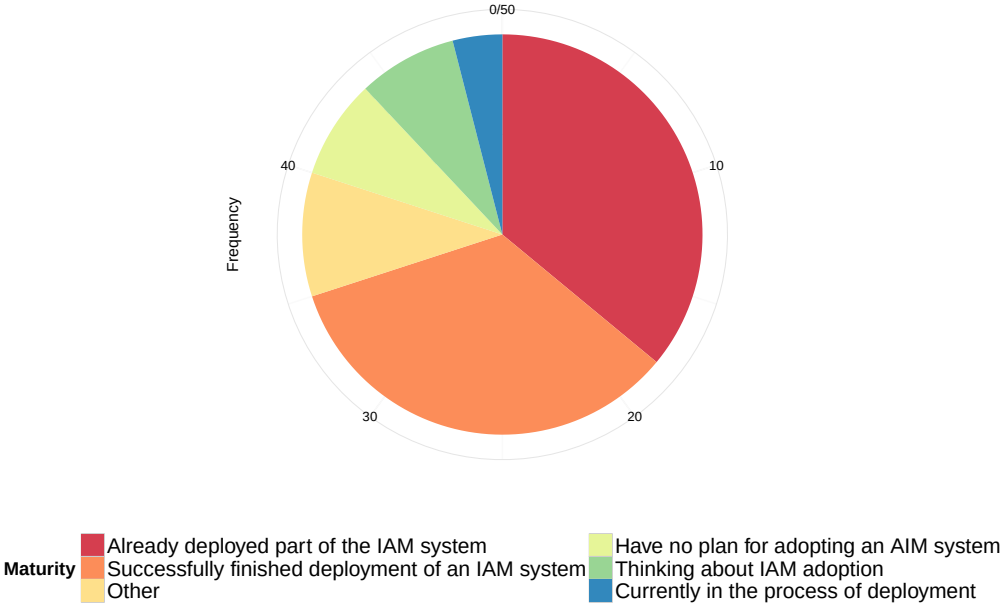


Figure 7: The state of IdM adoption in participants' organization

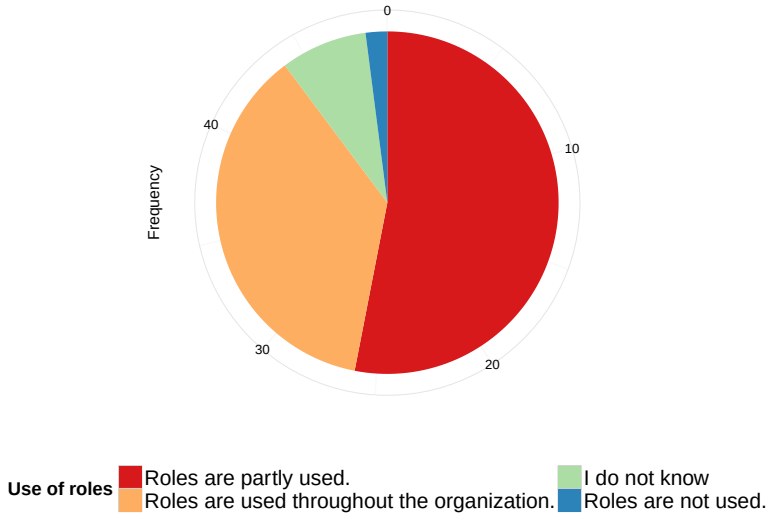


Figure 8: The use of roles in participants organization

data is generated in various ways for the reviewers such as using an AIM system, home-grown system, or manually. Using this question, we collected quantitative data on how access list generation is done in participants' company 12

Use of communication channels: To confirm and extend the list of communication

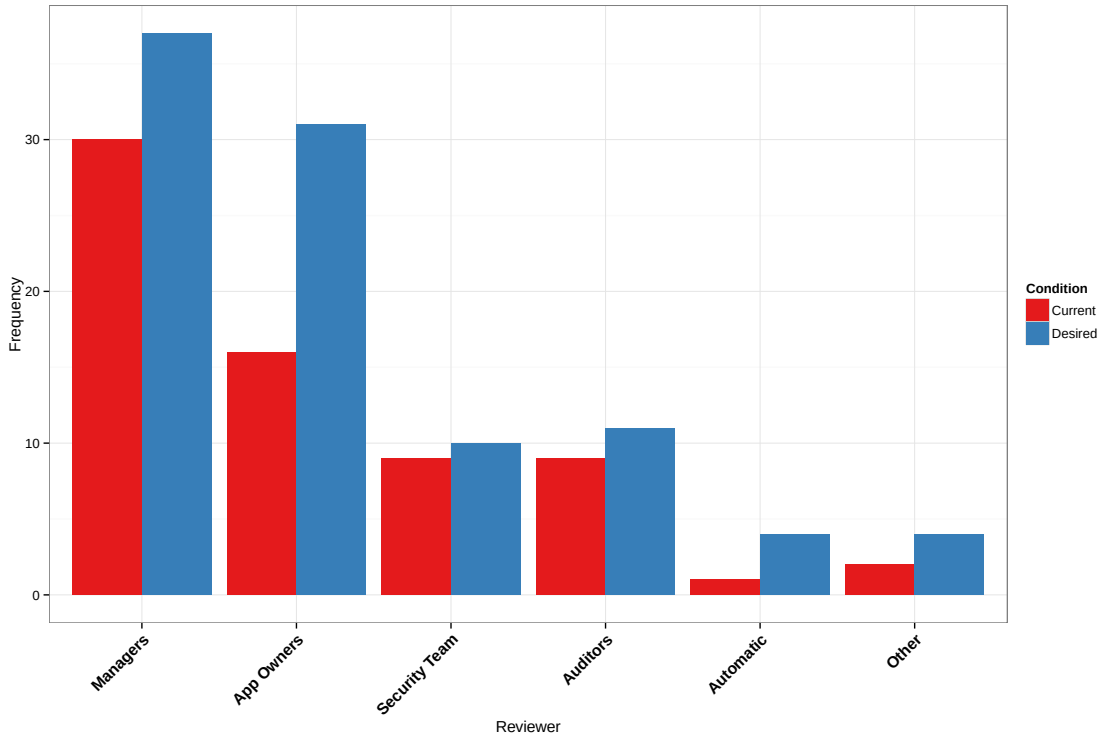


Figure 9: Participants' opinion on how access review should be performed

channels used during the review, we asked participants about the possible communications between various stakeholders involved in the access review activity. This result is summarized in Figure 13:

Those participants who provided further feedback, indicated the following communications might happen during access review:

- There is no need to communicate if the manager has access to identities and entitlements directly on the UI
- A recertification team is in place to monitor and help if needed
- Manager needs to discuss with users if there is a business need for the access

9 Information required for reviwing access

During our interview study, we identified a set of artifacts that are part of access review context. In the survey, our goal was to identify the importance of each artifact from the view point of participants. Therefore, we asked participants to rate the importance of each artifact on a five point likert scale. We show the summary of results in Figure 14.

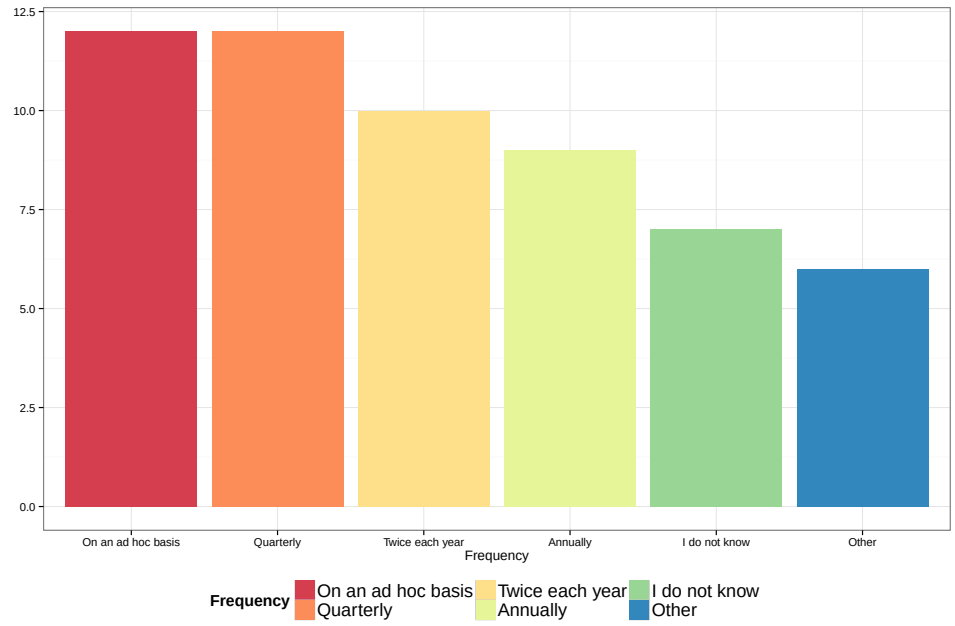


Figure 10: Frequency of performing access review

Furthermore, participants suggested other useful artifacts for access review:

- Identity attributes of the user: while we provided job function, other identity attributes such as location might be important.
- Violation of SoD rules was mentioned by two participants
- Employee feedback on his/her access before the review goes to the manager. For example, employees can first select the access they no longer need before the review goes to the manager this is very valuable information.
- One participant pointed to further uses of historical information: "The dates changes were made to users' access can be useful. For example: Changes in the last quarter; Changes made to a system during the same timeframe as a security breach; A batch of changes made during a reorganization may need a different level of review than day to day changes."
- The categorized list of users were also mentioned by a participant. He said focusing on specific types of users such as current employees, consultants, contractors, vendors, etc. can be useful. Also a list of employees who have departed since the last review is described as useful.
- Access end dates for temporary access

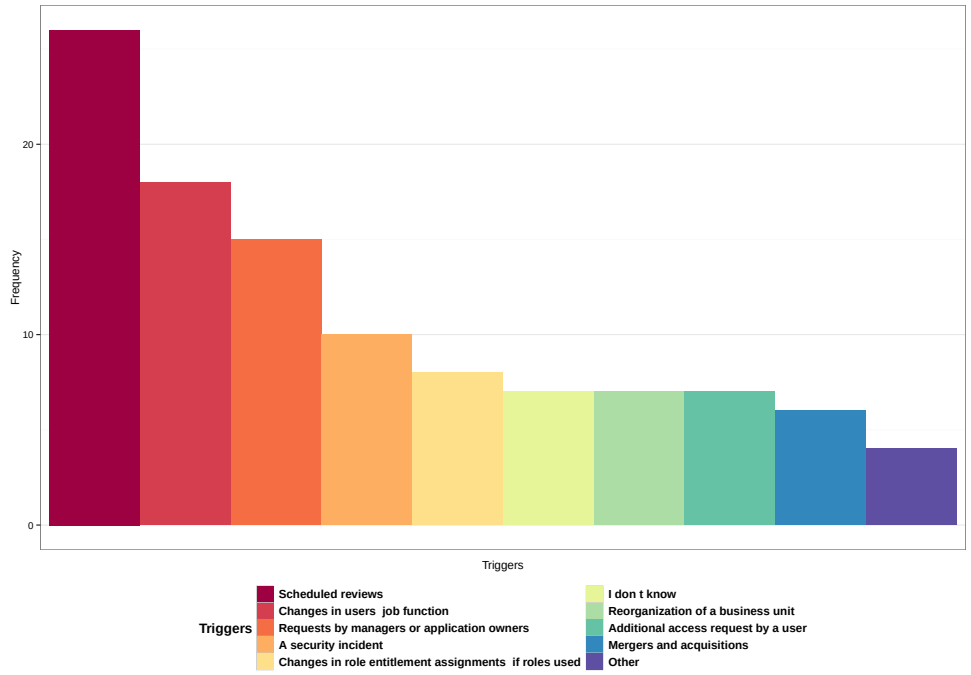


Figure 11: Overview of what triggers ad-hoc access reviews

- Another participants was noted that user's project is more important than his job title, or department. He said that in his company users are teamed-up according to their project.
- Entitlement owner
- Classification of the entitlement (Participant was working in Government sector)

We then asked participants that during access review, what they are particularly looking for as an indication of risk. We listed 10 risk indicators that were inferred from interview study results, and we gave participant the option of specifying it themselves. The summary of participants' responses is shown in Figure 15.

Participants further elaborated their responses:

- One participant mentioned: *"The number of users who have an entitlement is more likely an indication of how commonly it is needed; rather than any indication of risk."*
- Another participant said the classification based on the criticality of application is useful, but not enough: *"I would say the classification of entitlements or data is a much better indicator of risk than the above. Access to a Sox application is maybe more high risk than a non-sox application but what if they only have the*

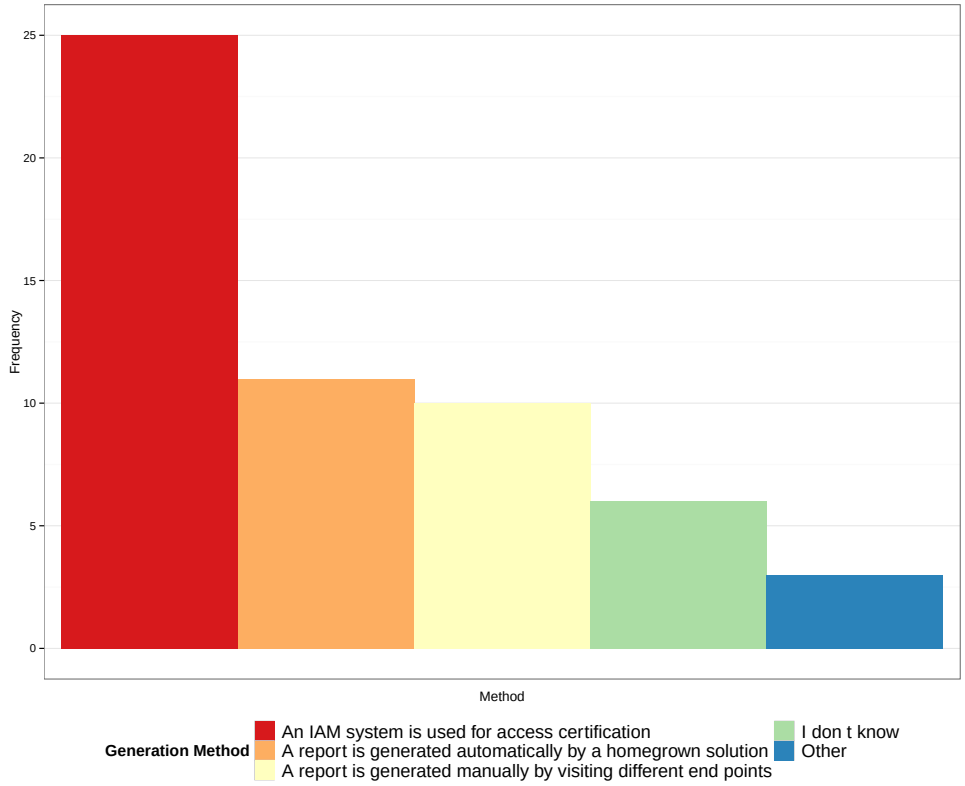


Figure 12: Overview of what triggers ad-hoc access reviews

ability to submit a PO in the Sox system. Far better to classify entitlements and then looks at what a user has. They have 500 entitlements I don't care...they have 500 Security Admin entitlements I do care."

- One participants noted that whether an entitlement is actually used or not is an important indicator: *"An entitlement that has been NOT actually used by the user to access the system could indicate an excess/unneeded entitlement or a recently granted entitlement."*
- The entitlements that are still associated with users after their expirey date
- One participant sais the SoD violations are not necessary risky, and might be due to something like holidays. But *"may occur only of they are visible and people are aware of the violation."*

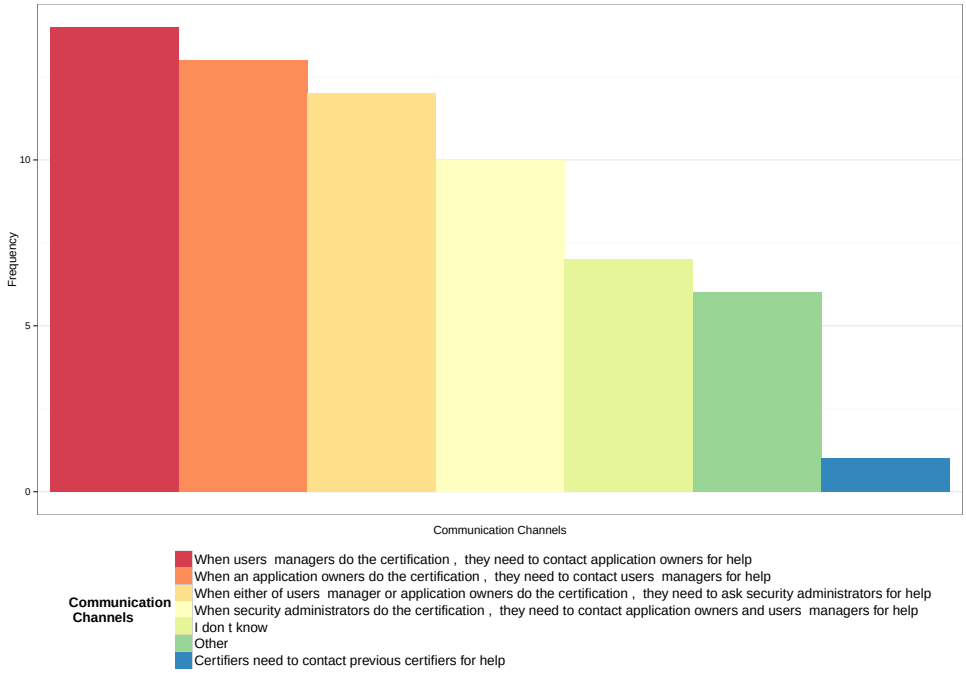


Figure 13: Communication Channels Used in Access Review

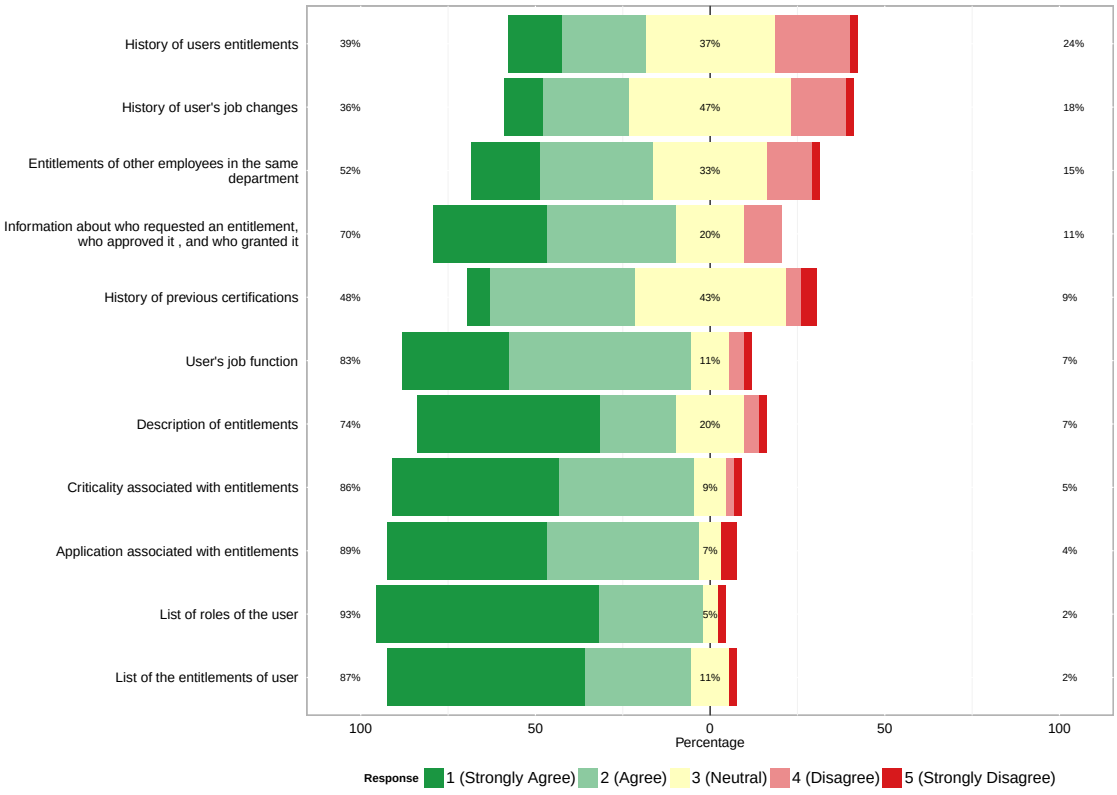


Figure 14: Usefulness of information during access review

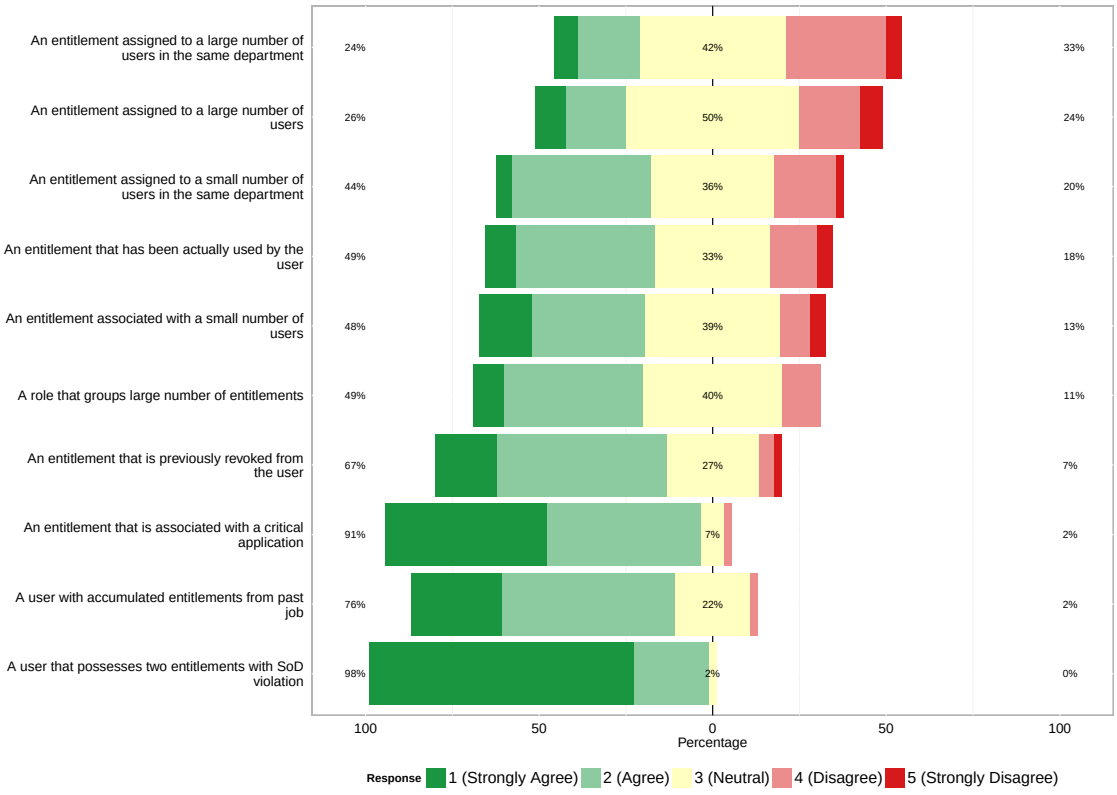
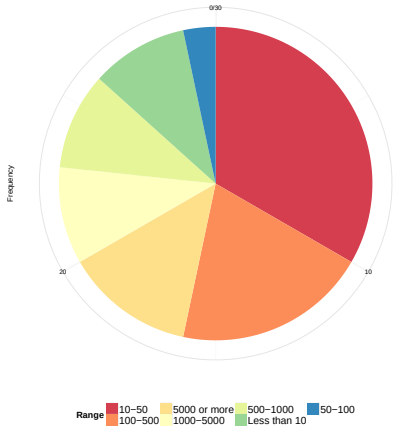
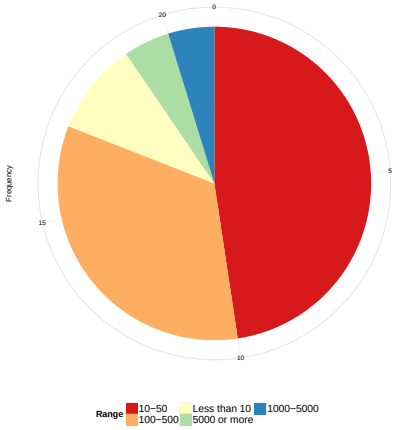


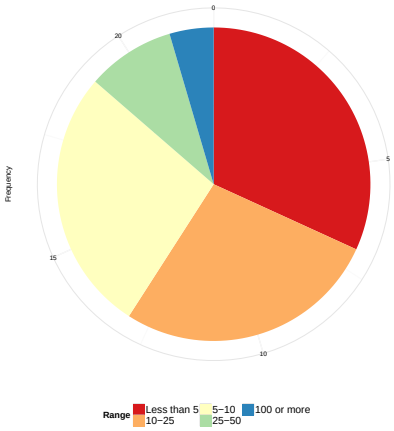
Figure 15: Risk indicators during access review



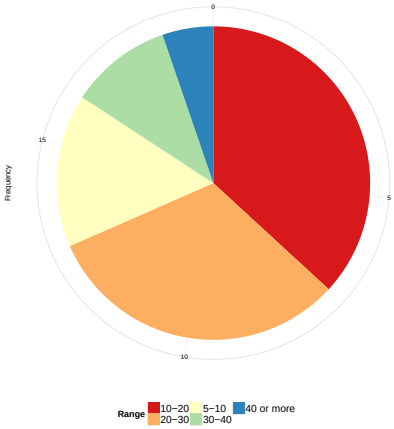
(a) Number of Applications



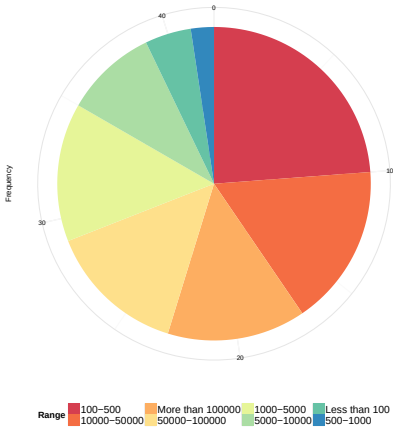
(b) Number of Entitlements Per User



(c) Number of roles per user



(d) Number of certifications per manager



(e) Number of users

Figure 16: Statistics on the number of various access review related entities