Privacy Audit—Methodology and Related Considerations

Auditors should consider key risk and control points when performing privacy audits. The following methodology draws heavily on concepts presented in ISO 31000:2009 Risk management—Principles and guidelines.

WHY CONDUCT A PRIVACY AUDIT?
Before considering the details of the privacy audit methodology, it is important to consider the reasons for conducting a privacy audit and the difference between confidentiality and privacy.

The objective of a privacy audit is to assess an organization’s privacy protection posture against any legislative/regulatory requirements or international best practices and to review compliance with the organization’s own privacy-related policies. The scope involves evaluating procedures undertaken by an organization throughout the typical information life-cycle phases: how information is created or received, distributed, used, maintained and eventually disposed of. As information and data have transformed from being scarce to superabundant, the privacy audit presents the status of risk associated with potential information misuse and recommends initiatives that can limit an organization’s liability or reputational risk.

THE DIFFERENCE BETWEEN CONFIDENTIALITY AND PRIVACY
Although frequently used interchangeably, confidentiality and privacy have distinct meanings. In this context, confidentiality can be referred to as the protection of information sharing without the express consent of the owner. Privacy, on the other hand, is freedom from intrusion into private matters. For example, external consultants working on a project within the organization might have access to private information (e.g., human resources records, customer databases), but they should not share this information with any other party as an expectation of maintaining confidentiality. At an individual level, privacy is guaranteed by the United Nations’ Universal Declaration of Human Rights (Article 12): “No one shall be subjected to arbitrary interference with his privacy...” and “Everyone has the right to the protection of the law against such interference or attacks.” In today’s world, companies act more or less with a notion of “corporate personhood,” that is, they can own assets, including intellectual properties, and engage in contractual relationships. Therefore, the concept of privacy can be easily imagined to be extended to corporations as well.

PRIVACY AUDIT METHODOLOGY
The high-level steps of the methodology that can be adopted to conduct a privacy audit are illustrated in figure 1.

The related considerations for each step are as follows:
- Establish context—A key challenge in any privacy-related discussion is that it is a very subjective phenomenon. A substantial amount of grey area always creeps in whenever attempts are made to define privacy, as there is no

![Figure 1—Privacy Audit Methodology Based on ISO 31000:2009](image_url)
universally agreed-upon understanding. The interpretation may vary significantly by country, culture or organization. For instance, most organizations nowadays set up a banner notification on computer login screens about monitoring the activities of the user and deploy some sort of technical tools on their network for this task. However, it is debatable to what extent the organization can utilize these data. Some argue that monitoring data (e.g., search terms, web sites visited, products purchased) on an organization’s resources (e.g., computer, Internet) during official working hours is not a violation of privacy, even if the company sells these data to an external party. Others term such actions as intrusion of privacy. The paramount question of who is the data owner (the company that collected the data or the individual[s] who produced the data) is given a fair amount of consideration. It is imperative for auditors to ensure that all stakeholders are aligned to the criteria used and the outcome of the proposed privacy audit.

- **Identify privacy risk**—The next step is to identify privacy-related risk by utilizing the usual risk identification tools, techniques and methods. Although listing all possible privacy risk is beyond the scope of this article and may not be practical, the following emerging risk areas should be part of this step:
  - Operating model—Hosted computer solutions (cloud computing) are increasingly considered by corporations. Without a reasonable degree of research, judgments are swiftly promulgated about the perceived evils of the hosted solutions. Auditors should objectively review the associated risk and assign the risk rating accordingly, keeping in mind that the concept of hosted solutions is neither novel nor abstract. Furthermore, cloud computing is not inherently bad news for privacy concerns. Such concerns are based on the unfounded belief that data kept in-house are somehow more secure. As a matter of fact, the security of data is dependent upon the security measures utilized by the organization and not on location—in-house or in the cloud.
  - Social media—Social media has provided an excellent way for companies to communicate with their customers and stakeholders on a timely basis. However, as is possible for personal social media accounts where information from different sources can be aggregated to reveal sensitive information, it may be possible for companies to be publishing seemingly innocuous information, but when combined or correlated with other sources, the information disclosed is private.
  - Mobile devices—The skyrocketing ownership of smart mobile devices has given rise to security concerns related to bring your own device (BYOD). From a privacy perspective, the following points are worth extra consideration:
    - Location data—The integration of navigation systems in the inherent cell-tower triangulation position system has raised some genuine privacy concerns. Geolocation data from mobile devices are considered to be sensitive. These data can be used for (unwanted) marketing to consumers based on location or for tracking the movement of users. Different guidelines are being developed to address the privacy of location-based data.
    - Hardware identifiers—Mobile apps can access unique hardware identifiers for marketing and other communication purposes to the consumer. Permission for such tracking might not have been explicitly granted by the owner of the device.
    - Personal utilities or games—Some mobile apps can gain unwarranted access to the utilities on the phone, which are not required for the intended purpose of installing the application.
  - Big data—The rapid enhancements in data collection and analytics technologies are resulting inversely in privacy erosion. Sophisticated tools can correlate data from different sources to identify personal or private information. The data warehouse created to analyze and
provide business benefits can also result in unintended leakage of private information.
– Conflict with other laws—Data privacy requirements can sometimes conflict with other laws, e.g., data retention laws.

**Analyze privacy risk**—Risk analysis predominantly consists of performing two steps:
1. Assign inherent risk rating.
2. Evaluate implemented controls.

Inherent risk rating can be assigned to each risk using an impact/consequence and probability matrix (see example in figure 2).

The effectiveness and efficiency of implemented controls should be assessed to evaluate the degree of risk mitigation. Examples of privacy controls that an organization may have or may wish to implement include, but are not limited to:
– Privacy policy—A policy should be documented, approved and communicated to all employees and stakeholders. In addition to taking any regulatory requirements into consideration, the policy should disclose management's intention on information collection and its subsequent usage.
– Database privacy controls—Cell suppression, partitioning, noise and perturbation are some of the techniques that can be used to mitigate risk associated with inference and aggregation attacks. In these kinds of attacks, information from different sources (e.g., online voter registration records, phone records, social network sites) is linked to disclose private information. For instance, a privacy enthusiast and researcher revealed the private health records of a governor of a US state using publicly available databases in a quintessential reidentification attack. Techniques such as privacy integrated queries (PINQ) could be used to provide privacy for underlying records.
– Cryptography—As required by several standards, including the Payment Card Industry Data Security Standard (PCI DSS), all personally identifiable information (PII) has to be stored in an encrypted format to prevent misuse or unauthorized access to such information.

<table>
<thead>
<tr>
<th>Probability</th>
<th>Consequence/Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>5—Definitely</td>
<td>Moderate risk</td>
</tr>
<tr>
<td>4—Likely</td>
<td>Moderate risk</td>
</tr>
<tr>
<td>3—Possible</td>
<td>Low risk</td>
</tr>
<tr>
<td>2—Unlikely</td>
<td>Low risk</td>
</tr>
<tr>
<td>1—Rare</td>
<td>Low risk</td>
</tr>
</tbody>
</table>

**Figure 2**—Inherent Risk Rating Matrix

![Inherent Risk Rating Matrix](image)

**Figure 3**—Privacy Residual Risk Calculation

![Privacy Residual Risk Calculation](image)
• Evaluate privacy risk—The residual risk is calculated based on inherent risk and control ratings. Residual risk is the level of risk that remains after taking into account all existing controls. Figure 3 shows a suggested equation for residual risk calculation.

• Manage privacy risk—This step is primarily performed by management, and the auditor’s role generally is to ascertain the adequacy of the steps taken to mitigate risk. Using residual risk rating as a basis, risk management initiatives can be identified. Such initiatives might include strengthening the current controls or implementing new controls to mitigate privacy-related risk. There are several forms of risk management, such as avoidance, transfer or reduction to an acceptable level, after taking into consideration the cost vs. benefit of the risk treatment.

• Communicate and consult—Periodic reports should be provided to management, the audit committee and any other stakeholder during each phase of the methodology. Any major areas of concern should be brought to management’s attention immediately.

• Monitor and review—The performance of the privacy risk management system should be continuously monitored. Regulatory requirements, internal processes and business processes might change, which, in turn, could affect privacy risk management practices. Appropriate monitoring and review processes should be completed throughout the risk management process to ensure that all decisions are made based upon current and up-to-date information.

CONCLUSION

The notion and understanding of privacy will continue to evolve. Data collection and utilization have already been, and continue to be, even more pervasive, in some cases with the individual’s consent, but in many cases without the individual’s knowledge. Debates will continue about privacy on one hand and efficiency and convenience on the other. New or updated regulatory requirements are expected to emerge as well.

In this ever-changing scenario, auditors should establish and follow a comprehensive privacy audit methodology to ensure that their organizations are not inadvertently exposed to any undesired risk. Furthermore, steps should be taken to ensure that all privacy-related risk is minimized to an acceptable level. Auditors should also be wary of emerging technological trends and their impact on privacy. Consideration should be given to include privacy audit in the annual audit plan, and reports should be provided on a periodic basis to all stakeholders.

REFERENCES


Enright, Keith P.; Privacy Audit Checklist, http://cyber.law.harvard.edu/ecommerce/privacyaudit.html

Determann, Lothar; “Data Privacy in the Cloud: A Dozen Myths and Facts,” The Computer and Internet Lawyer, vol. 28, no. 11, November 2011


ENDNOTES


