Auditing Data Privacy

I consider myself a private person, so, naturally, this tendency is reflected in my online profile. I do have Facebook and Instagram accounts, but these were initially created to monitor my children's online activity and I rarely, if ever, post on them. I also have Twitter and LinkedIn accounts, which I use to post technology-, audit- and cybersecurity-related news. My only real online presence is reflected in this column, related blogs and anything ISACA® posts to promote same.

So, is my privacy maintained? With the advent of machine learning, it is possible to classify text in any number of ways. Web services[1] exist that use labeled training texts to determine the mood, gender, age and personality[2] of content authors. I have fed some of my previous columns into the site and some of the classifications are scarily accurate.

Privacy is the right of an individual to trust that others will appropriately and respectfully use, store, share and dispose of his/her associated personal and sensitive information within the context and according to the purposes for which it was collected or derived.[3] The context is important. I am aware that this column is posted online and does not require a password to access, therefore, I cannot reasonably expect my privacy to be fully maintained.

However, now consider your last audit report. How would you feel if it was used to classify your personality? Could your next promotion be decided by artificial intelligence (AI)? Is this acceptable? Probably not without consent. So how can we audit to help mitigate this and other privacy risk?

In previous columns,[4,5] I advocated the use of an ISACA paper on creating audit programs.[6] This article will once again apply this process to build an audit program for privacy for your organization.

Determine Audit Subject

The first thing to establish is the audit subject. What does privacy mean in your enterprise? If there are distinct categories of data in use for different areas of the business, they should probably be recorded as separate audit universe items. Fundamentally, though, when considering privacy, the data can be broken down to data stored on customers and employees (the right of an individual).[7] Besides databases, files and documents, it is important to also consider where the data are stored and/or from where they are derived, including:[8]

- Social media
- Cloud computing
- Mobile devices
- Big data analytics/machine learning/AI
- Internet of Things (IoT)
- Personal devices (bring your own device [BYOD])
- Tracking/surveillance technologies—drones, radio frequency identification (RFID) tags, closed circuit television (CCTV), global positioning satellite (GPS) devices

The key is to consider categories of data and determine the audit subject(s). You need to answer the key question: What are you auditing?

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2J4c5QI

Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and Implementer, CFE, CPTE, DipFM, ITIL Foundation, Six Sigma Green Belt
Is the group IT audit manager with An Post (the Irish Post Office based in Dublin, Ireland) and has 30 years of experience in all aspects of information systems. Cooke has served on several ISACA committees and is a current member of ISACA's CGEIT® Exam Item Development Working Group. He is the community leader for the Oracle Databases, SQL Server Databases, and Audit Tools and Techniques discussions in the ISACA Knowledge Center. Cooke supported the update of the *CISA® Review Manual* for the 2016 job practices and was a subject matter expert for ISACA's CISA® and CRISC™ Online Review Courses. He is the recipient of the 2017 John W. Lainhart IV Common Body of Knowledge Award for contributions to the development and enhancement of ISACA publications and certification training modules. He welcomes comments or suggestions for articles via email (Ian_J_Cooke@hotmail.com), Twitter (@COOKEI), or on the Audit Tools and Techniques topic in the ISACA Knowledge Center. Opinions expressed are his own and do not necessarily represent the views of An Post.

Define Audit Objective

Once you have decided what you are auditing, you need to establish the objective of the audit. Why are you auditing it? From an auditor's perspective, it is advisable to adopt a risk-based view and define the objectives accordingly:

- First, consider the seven categories of privacy:
  1. Privacy of person
  2. Privacy of behavior and action
  3. Privacy of communication
  4. Privacy of data and image (information)
  5. Privacy of thoughts and feelings
  6. Privacy of location and space (territorial)
  7. Privacy of association[9]
- Next, consider the risk across the seven categories (**figure 1**).[10] Privacy risk can lead to adverse publicity and reputational damage resulting in customer and economic loss, including fines.
- Finally, consider the audit objectives. This is likely to include compliance to laws and regulations (e.g., the US Health Insurance Portability and Accountability Act [HIPAA],[11] the EU General Data Protection Regulation [GDPR][12, 13]) and possibly the use of a framework such as International Organization for Standardization (ISO) and International Electrotechnical Commission's (IEC) ISO/IEC 29100:2011 *Information technology—Security techniques—Privacy framework*.[14] However, I also recommend considering the ISACA Privacy Principles (**figure 2**) for Audit Objectives. Why? Because the principles were developed by considering privacy laws, standards, frameworks and principles from around the world. They can, therefore, act as an overarching framework and will likely cover all privacy objectives.

Set Audit Scope

When you have defined the objectives of the audit, you should use a scoping process to identify the actual data that need to be audited. In other words, what are the limits to the audit? This could include data in a specific application, process, location or stored by certain devices. Again, this should be risk based.

Perform Pre-Audit Planning

Now that you have identified the risk, it should be evaluated to determine its significance. Conducting a risk assessment is critical in setting the final scope of a risk-based audit. The more significant the risk, the greater the need for assurance. Sample assurance considerations based upon the privacy principles include:[15]

Figure 1—Examples of Privacy Risk

Privacy Category	Example Risk
Privacy of behavior and action	**Social media** contains information, images, video and audio that reveal personal activities, orientations and preferences, many of which are sensitive in nature and can impact the data subjects.
Privacy of thoughts and feelings	**Big data analytics** has the potential to take large amounts of data and reveal the thoughts or feelings of specific individuals based on data they provide or others provide about them. Such insights can result in negative impact if actions are taken because of the analytics findings.
Privacy of location and space (territorial)	**Privately owned computing devices** that are used for business activities may also be able to record images and audio. Such images and audio create privacy risk if the devices are also used to perform business activities within the workplace.

Source: Adopted from ISACA, *ISACA Privacy Principles and Program Management Guide*, USA, 2016. Reprinted with permission.

Figure 2—ISACA Privacy Principles	
Principle Number	**Principle**
1	Choice and consent
2	Legitimate purpose specification and use limitation
3	Personal information and sensitive information life cycle
4	Accuracy and quality
5	Openness, transparency and notice
6	Individual participation
7	Accountability
8	Security safeguards
9	Monitoring, measuring and reporting
10	Preventing harm
11	Third-party/vendor management
12	Breach management
13	Security and privacy by design
14	Free flow of information and legitimate restriction

Source: ISACA, *ISACA Privacy Principles and Program Management Guide*, USA, 2016. Reprinted with permission.

- **Choice and consent**—Does the enterprise ensure that appropriate consent has been obtained prior to the transfer of personal information to other jurisdictions?
- **Legitimate purpose specification and use limitation**—Does the enterprise specify the purpose(s) for which personal information is collected?
- **Personal information and sensitive information life cycle**—Does the enterprise retain personal information for only as long as necessary?
- **Accuracy and quality**—Does the enterprise implement practices and processes to ensure that personal information is accurate, complete and up to date?
- **Openness, transparency and notice**—Does the enterprise provide clear and easily accessible information about its privacy policies and practices?
- **Individual participation**—Does the enterprise provide data subjects a process to access their personal information?
- **Accountability**—Does the enterprise assign roles, responsibility, accountability and authority for performing privacy processes?
- **Security safeguards**—Does the enterprise ensure that appropriate security safeguards are in place for all personal information?
- **Monitoring, measuring and reporting**—Does the enterprise report compliance with policies, standards and laws?
- **Preventing harm**—Does the enterprise establish processes to mitigate any personal harms that may occur to data subjects?
- **Third-party/vendor management**—Does the enterprise implement governance processes to ensure the appropriate protections and use of personal information that are transferred to third parties?
- **Breach management**—Has the enterprise established a documented policy and supporting procedure for identifying, escalating and reporting incidents?
- **Security and privacy by design**—Does the enterprise ensure executive support for the identification of personal information and privacy risk within enterprise events?
- **Free flow of information and legitimate restriction**—Does the enterprise follow the requirements of applicable data protection

authorities for the transfer of personal information across country borders?

Interviewing the auditee to inquire about activities or areas of concern that should be included in the scope of the engagement. Once the subject, objective and scope are defined, the audit team can identify the resources that will be needed to perform the audit work.[16]

> "IT IS IMPORTANT TO REMEMBER THAT SECURITY DOES NOT MEAN PRIVACY."

Determine Audit Procedures and Steps for Data Gathering

At this stage of the audit process, the audit team should have enough information to identify and select the audit approach or strategy and start developing the audit program.[17] You now have enough information to decide what documents you expect to see, what laws and regulations apply, the criteria, and whom you are going to interview. You do, however, need to define the testing steps. In the latter half of 2017, ISACA released an audit/assurance program that defines testing steps for data privacy.[18] As always, this should be considered a starting point and should be adjusted based upon risk and criteria that are relevant to the organization you are auditing. It is worth spending the time to consider the risk and the resulting need for assurance (**figure 3**).

Key testing steps in the audit program are security related. However, it is important to remember that security does not mean privacy. Confidentiality is preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information.[19] Privacy is a possible outcome of security.[20]

Figure 3—Assurance Consideration to Audit Program Mapping

Privacy Principle Number	Audit Program Sample Control
1	When personally identifiable information (PII) is obtained from individuals, consent is obtained.
2	Clear guidelines are in place to ensure the appropriate use and retention of data throughout the enterprise.
3	Clear guidelines are in place to ensure the appropriate use and retention of data throughout the enterprise.
4	Determine if the record management guideline describes the enterprise's strategy and procedures regarding maintenance, retention and destruction of records in accordance with all state and federal laws and regulations.
5	When PII is obtained from individuals, consent is obtained.
6	Purpose and scope/applicability of the record management process are clearly defined.
7	Roles and responsibilities of the people involved in the management of data governance for privacy, confidentiality and compliance for the enterprise have been clearly defined.
8	Appropriate data encryption standards are in place for data at rest, and appropriate awareness campaigns are conducted to train employees.
9	Awareness is accounted for and key metrics are utilized for conformance and compliance to required training.
10	Integration of privacy impact assessments (PIAs) is firmly established in the enterprise and proper tools and monitoring are in place for the validation of compliance.
11	Contractual language for third-party management of PII is appropriately included and agreed upon.
12	The breach escalation plan is in place to react to PII breaches.
13	Data deidentification across the enterprise is enforced appropriately through tools and automated means.
14	Global privacy policies and requirements have been modified to align with region- or country-specific requirements.

Conclusion

New and emerging technologies will enable enterprises to derive increased insight and, thus, value from data. This will, no doubt, provide competitive advantage. ISACA's Privacy Principles can be used as an overarching framework in conjunction with these technologies to provide assurance that an enterprise respects the privacy rights of an individual. Demonstrating this to those individuals will also provide a competitive advantage.

Endnotes

1 uClassify is a free machine learning web service. *https://www.uclassify.com/*
2 The Myers and Briggs Foundation, The Myers-Briggs Type Indicator, *www.myersbriggs.org/my-mbti-personality-type/mbti-basics/*
3 ISACA, *ISACA Privacy Principles and Program Management Guide*, USA, 2016, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ISACA-Privacy-Principles-and-Program-Management-Guide.aspx*
4 Cooke, I.; "Audit Programs," *ISACA® Journal*, vol. 4, 2017, *https://www.isaca.org/Journal/archives*
5 Cooke, I.; "Auditing Mobile Devices," *ISACA Journal*, vol. 6, 2017, *https://www.isaca.org/Journal/archives*
6 ISACA, *Information Systems Auditing: Tools and Techniques, Creating Audit Programs*, USA, 2016, *https://www.isaca.org/Knowledge-Center/Research/Documents/IS-auditing-creating-audit-programs_whp_eng_0316.pdf*
7 *Op cit* ISACA, *ISACA Privacy Principles and Program Management Guide*, p.11
8 *Ibid*. p. 31
9 *Ibid*. p. 28
10 *Ibid*. p. 31
11 Department of Health and Human Services, Health Insurance Portability and Accountability Act, USA, *https://www.hhs.gov/hipaa/index.html*
12 European Commission, 2018 Reform of EU Data Protection Rules, *https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en*
13 Herold, R.; "Using ISACA Privacy Principles for GDPR Compliance," *COBIT Focus*, August 2017, *www.isaca.org/COBIT/focus/Pages/using-isaca-privacy-principles-for-gdpr-compliance.aspx*
14 International Organization for Standardization, ISO/IEC 29100:2011, *Information technology—Security techniques—Privacy framework*, *https://www.iso.org/standard/45123.html*
15 *Op cit* ISACA, *ISACA Privacy Principles and Program Management Guide*, p. 44
16 ISACA, Audit Plan Activities: Step-By-Step, 2016, *https://www.isaca.org/cobit/documents/Audit-Plan-Activities_res_eng_0316.pdf*
17 *Ibid*.
18 ISACA, *IS Audit/Assurance Program, Data Privacy*, USA, 2017, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/data-privacy-audit-program.aspx*
19 *Op cit* ISACA, *ISACA Privacy Principles and Program Management Guide*, p. 13
20 *Ibid*.

Enjoying this article?

- Learn more about, discuss and collaborate on it audit tools and techniques in the Knowledge Center. *www.isaca.org/it-audit-tools-and-techniques*