IIA Bulletin

The Institute of Internal Auditors

Perspective for internal auditors on today's most urgent issues *January 2020*

International Data Privacy Day

Jan. 28 is International Data Privacy Day, which serves as an important reminder that internal audit leaders must be aware of and understand privacy-related regulations applicable to their organization, as well as their organizations' posture on data privacy. The growing list of regulations from jurisdictions around the world is making data privacy increasingly complex and dynamic. These regulations cover a wide range of issues including specific requirements related to data collection, management, storage, and usage.

For example, regulatory guidance on data privacy policies has existed for financial organizations that comply with the Gramm-Leach-Bliley Act (GLBA) for decades. Meanwhile, the California Consumer Privacy Act (CCPA) just went into effect on Jan. 1, 2020, yet lawmakers continue to make changes to the landmark legislation. Similarly, implementation of the European Union's Global Data Protection Regulations (GDPR) since its start date in May 2018 has played out somewhat differently than originally anticipated, leaving some organizations with more questions than answers.

Internal audit leaders should stay current on this volatile risk area (see resources on page 2) and incorporate audits focusing on data governance, data ethics, data management, and data privacy practices. Compiled below is a list of general questions designed to assist organizations who have yet to conduct an assessment on data privacy.

General questions to assess your organization's data privacy

The following are some general questions your internal audit department should ask to determine if your organization is properly addressing data privacy:

- How was data privacy identified in the most recent risk assessment?
- Who is designated as the organization's Data Protection Officer, or person responsible for data privacy and compliance?
- Who owns the organization's customer data privacy policy (policies)?
- Where does management maintain an inventory of the regulations its organization is subject to, and how is it kept up to date?

- Where does management maintain an inventory of all third parties who accept, process, or house data on the organization's behalf, and how is it kept up to date?
- Which programs and applications house sensitive data? Are there sufficient IT general controls, application controls, and network controls over them? Are these controls operating effectively?
- What other relevant controls (preventive and detective) are in place regarding data privacy? Are they operating effectively?
- Who is accountable for ensuring there is a documented process detailing what to do in the event of a data breach, and where does this documentation reside?

Six steps to a simple data privacy audit

While the activities performed during the data privacy audit will vary from organization to organization, the following example is an outline for internal auditors to use as they plan and perform a simple but valuable data privacy audit:

1. Gather inventory of:
   - All applicable regulations with privacy components.
   - All of your organization's data privacy policies (e.g., websites, mobile, mail, phone, email).
   - All of your third-party data privacy policies (those you redirect your clients to such as PayPal).
2. Compare all applicable privacy-related regulatory criteria to your organization's data privacy policies. Note any exceptions or gaps.
3. Compare all applicable third-party privacy policies to your organization's own data privacy policies. Note any inconsistencies.
4. Map the policy(s) that align with your organization's controls. Gaps will show potential higher risk areas.
5. Verify that what is outlined in the policy(s) is in practice (tied to specific processes and controls). Note any exceptions. Elements to validate include: What data is captured? What data is stored? How long is it stored? How is it used? Who is it sold to? Who has read access? Who has write access? How long is it retained? How is it destroyed? Make a note if any of these questions are not answered in your policy.
6. Validate controls. One simple test is to log on to an application that should adhere to your data privacy policy, then obtain and review the content regarding your activities along the way.

IIA RESOURCES

GTAGS

- Auditing Third-Party Risk Management

Practice Guides

- Understanding and Auditing Big Data

Internal Auditor magazine

- Six Data Privacy Predictions for 2020
- Privacy Law Puts California Consumers in Control
- GDPR's Global Reach
- A Matter of Privacy
- The Consumer's Data Anxiety
- Assurance in the Privacy Regulatory Age

Internal Audit Foundation

- Cybersecurity: What the Board of Directors Needs to Ask
- Privacy In The Age Of Big Data: Recognizing Threats, Defending Your Rights, And Protecting Your Family