Privacy Risk Management

Concerns about privacy risk have triggered a number of new privacy protection regulations: The US State of California Consumer Privacy Act (CCPA) went into effect on 1 January 2020, the Brazilian General Data Protection Law (LGPD) becomes effective in August 2020, China has completed the first draft of a personal information protection law, New Zealand's privacy law is likely to take effect in mid-2020, and the EU General Data Protection Regulation (GDPR) will be replaced as an applicable law in the United Kingdom at the end of 2020.[1] The increasing trend of privacy legislation exacerbates privacy risk, which is a trigger for privacy protection requirements and influences consumer trust and enterprise reputation. So, what is privacy risk? From what is privacy risk arising?

Andrea Tang, CIPP/E, ISO 27001 LA
Works at a Big Four organization and has working experience in providing data security and privacy services to financial institutions. This year, she has published a series of professional articles on the ISACA® WeChat official account, which has won wide attention, recognition and support from the ISACA China Technical Committee. Additionally, she has contributed to the *ISACA® Journal*, and the "ISACA China Digital IT Risk Framework" project and publication, which will be issued this year. As an active volunteer in the ISACA Beijing (China) Chapter, Tang was the winner of the outstanding young professional award in 2018-19. She has a passion for sharing the latest privacy trends and technology with experts around the world. Additionally, she has organized several successful knowledge-sharing events in the ISACA China community.

What Is Privacy Risk?

Privacy risk is the likelihood that individuals will experience problems resulting from data processing, and the impact of these problems should they occur.[2] Privacy risk includes but is not limited to technical measures that lack appropriate safeguards, social media attacks, mobile malware, third-party access, negligence resulting from improper configuration, outdated security software, social engineering and lack of encryption.

According to article 4 of GDPR, data processing is a set of operations including but not limited to the collection, storage, adaptation or alteration, disclosure by transmission, and dissemination of data.[3] ISACA® provides a data life cycle model that can be taken into consideration when building a data inventory (**figure 1**).[4]

Privacy risk can exist throughout the data life cycle, so it is important to manage and govern data properly. A number of privacy risk management activities can be undertaken during the data life cycle.[5] Designing a privacy risk management framework is the first step to ensure data validation and data protection, to monitor and control data, and to comply with all applicable laws and regulations.

Creating and Implementing a Privacy Risk Management Framework

The globally recognized COBIT® 2019 framework can serve as a foundation to ensure effective enterprise governance of information and technology (EGIT).[6] It can help an enterprise govern data, implement internal and external security, and determine the components needed from other frameworks. It is a useful tool for implementing a privacy risk management framework, particularly by focusing on the four management domains (**figure 2**):

1. Align, Plan and Organize (APO)
2. Build, Acquire and Implement (BAI)
3. Deliver, Service and Support (DSS)
4. Monitor, Evaluate and Assess (MEA)

Figure 1—Data Life Cycle Mapping With Data Inventory Considerations

PLAN/DESIGN	BUILD/ACQUIRE	STORE	USE	SHARE	ARCHIVE/ DESTROY
What is the context and purpose of the repository?	Where are the data moving from and to?	What kind of information is in the repository?	How is the information being used?	Where will the data flow (from country to country)?	What data are currently being retained, how and where?
Who is the owner of the repository?	How much data are in the repository?	In which country or countries are the data stored?	From which country or countries is the data accessed?	Are the data shared with third parties? Are they controllers, joint controllers or processors?	What are the scenarios that would require data retention or destroy?
Is the data dictionary design compatible with different systems?	Is this a paper or electronic repository?	Are there any technical safeguard measures for data storage?	Are the data applied to automated decision making?	Is the data sharing obtained with explicit consent from data subjects?	Do the technical measures taken for data destruction guarantee they are irrecoverable?
Is the data dictionary design compliant with laws and regulations?	Are the data structured or unstructured?	Are the data stored in the cloud?	Is there any legal basis provided for the data usage?	Is there any DPIA conducted for data sharing?	Are the data archived/destroyed in compliance with laws and regulations?

Figure 2—Mapping to COBIT®

Privacy Risk Management Framework	COBIT® 2019
Stage 1: Establish privacy governance	BAI01 Managed programs BAI11 Managed projects
Stage 1-1: Define privacy governance goals	APO01 Managed information and technology (I&T) management framework APO02 Managed strategy APO03 Managed enterprise architecture
Stage 1-2: Establish enterprise privacy risk management framework	APO04 Managed innovation APO05 Managed portfolio
Stage 1-3: Realize the benefits of privacy risk management	APO06 Managed budget and costs APO07 Managed human resources APO08 Managed relationships
Stage 2: Conduct privacy risk management activities Stage 2-1: Define privacy risk assessment framework	APO12 Managed risk
Stage 2-2: Conduct privacy risk assessments Stage 2-2-1: Vendor/third-party risk assessments Stage 2-2-2: Data breach readiness assessments	APO09 Managed service agreements APO10 Managed vendors DSS02 Managed service requests and incidents
Stage 3: Implement risk response Stage 3-1: Establish response procedures for privacy risk	DSS03 Managed problems
Stage 3-2: Response to privacy risk	DSS04 Managed continuity
Stage 3-3: Evaluate privacy risk response	MEA01 Managed performance and conformance monitoring MEA02 Managed system of internal control MEA03 Managed compliance with external requirements MEA04 Managed assurance

> SPECIFIC AND CLEAR COMMUNICATION ABOUT THE ENTERPRISE'S APPROACH IS KEY TO OBTAINING SUPPORT FOR THE PRIVACY RISK MANAGEMENT PROGRAM.

Stage 1: Establish Privacy Governance

The US National Institute of Standards and Technology's (NIST) Privacy Framework is intended to assist organizations in communicating and organizing privacy risk and rationalizing privacy to build or evaluate a privacy governance program. The NIST Privacy Framework defines privacy governance as govern/develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.[7] In this stage, the enterprise could do the tasks outlined in **figure 3**.

Stage 1-1: Define Privacy Governance Goals

The first step is for the enterprise to create a privacy vision and mission statement. Stakeholders should take market expectations into consideration, establish an overall privacy risk management strategy, define the scope of privacy governance by identifying applicable personal data protection laws and regulations, structure a privacy team, and define a privacy risk tolerance level.

Specific and clear communication about the enterprise's approach is key to obtaining support for the privacy risk management program. But it should be noted that there is no one-size-fits-all strategy. The enterprise must consider its own circumstances and the business environment when adopting a privacy strategy.

Stage 1-2: Establish Enterprise Privacy Risk Management Framework

An enterprise privacy risk management framework consists of the following elements:

- **Purpose**—Explain privacy governance goals in detail.
- **Scope**—Define the personal data required to be protected and the internal policies to be followed.
- **Risk**—Identify potential risk factors, vulnerabilities and threats related to data processing activities.
- **Responsibilities**—Set up a privacy committee consisting of identified stakeholders, specify the role of each department (e.g., which executives must approve funding for the privacy team), establish the role of the data protection officer, support privacy initiatives such as training and awareness, and hold employees accountable for following all privacy policies and procedures.
- **Processes**—Establish privacy risk management processes.

Stage 1-3: Realize the Benefits of Privacy Risk Management

A privacy risk management framework is intended to help enterprises weigh the benefits of data processing against the risk of doing so and determine which risk response measures should be adopted.

Stage 2: Conduct Privacy Risk Management Activities

NIST also states that a privacy risk management framework is intended to help enterprises weigh the benefits of data processing against the risk of doing so and determine which risk response measures should be adopted.[8] In this stage, enterprises could conduct the tasks listed in **figure 4**.

Figure 3—Creating and Implementing a Privacy Risk Management Framework—Stage 1: Establish Privacy Governance

Stage 1-1 Define privacy governance goals	**Stage 1-2** Establish enterprise privacy risk management framework	**Stage 1-3** Realize the benefits of privacy risk management

Figure 4—Creating and Implementing a Privacy Risk Management Framework—Stage 2: Conduct Privacy Risk Management Activities

Stage 2-1 Define Privacy Risk Assessment Framework	**Stage 2-2** Conduct Privacy Risk Assessments

Stage 2-1: Define Privacy Risk Assessment Framework

A privacy risk assessment determines whether an enterprise is in compliance with applicable laws and regulations, industry standards, and internal policies and procedures. Based on a survey by the International Association of Privacy Professionals (IAPP) and TrustArc,[9] the vendor/third-party risk assessment is the most common type of assessment conducted (**figures 5** and **6**). Also common are data protection impact assessments (DPIAs), privacy impact assessments (PIAs) and legitimate interest assessments (LIAs).

A DPIA is designed to identify risk arising from the processing of personal data and to minimize this risk as much and as early as possible.[10] DPIAs can help prioritize risk, allowing resources to be concentrated on the domain with the highest risk and the greatest potential damage in order to mitigate that risk.

A PIA is an analysis of the risk factors associated with processing personal information in relation to a project, product or service.[11] PIAs provide remediation measures to avoid or mitigate risk. In addition to COBIT 2019, several others are available to help enterprises address privacy risk:

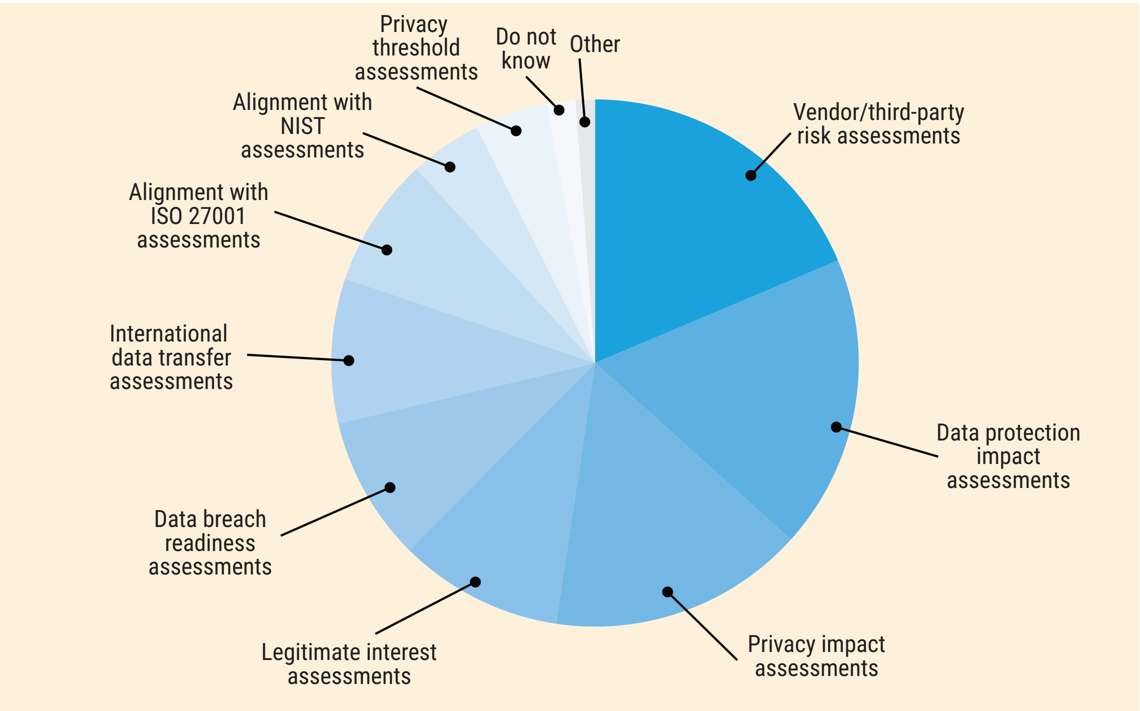
- **NIST Privacy Framework**—Version 1.0 of the NIST Privacy Framework,[12] released in January 2020, is a tool to assess and mitigate privacy risk, implement privacy engineering, and design products and services to protect individuals' privacy by providing a set of activities and outcomes that enables enterprise stakeholders to discuss managing privacy risk (**figure 7**).
- **International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standard ISO/IEC 27701**—This first global privacy standard, released in August 2019, provides a risk-based framework for a privacy risk management system.[13] It helps enterprises translate principles-based legal requirements into technical privacy controls that can be implemented in tandem with security controls (**figure 8**).

Figure 5—IAPP Survey: Privacy Risk Assessments

Which of the Following Types of Privacy Assessments Does Your Organization Conduct?

	Overall	US	EU+UK	Regulated	Unregulated
Vendor/third-party risk assessments	63%	78%	52%	69%	69%
Data protection impact assessments	61%	53%	81%	60%	65%
Privacy impact assessments	53%	55%	45%	57%	49%
Legitimate interest assessments	34%	24%	53%	32%	41%
Data breach readiness assessments	30%	38%	26%	33%	30%
International data transfer assessments	30%	27%	37%	29%	35%
Alignment with ISO 27001 assessments	27%	26%	33%	25%	31%
Alignment with NIST assessments	15%	28%	5%	19%	15%
Privacy threshold assessments	15%	16%	15%	14%	17%
Do not know	6%	4%	3%	5%	3%
Other	4%	4%	2%	3%	5%

Figure 6—IAPP Survey: Privacy Risk Assessments (Pie Chart Analysis)



Source: Adapted from International Association of Privacy Professionals (IAPP) and TrustArc, *Measuring Privacy Operations 2019: Cookies, Local vs. Global Compliance, DSARs and More*, USA, 2019

Figure 7—Mapping to NIST Privacy Framework

Privacy Risk Management Framework	NIST Privacy Framework
Stage 1: Establish privacy governance	Governance policies, processes and procedures (GV.PO-P)
Stage 1-1: Define privacy governance goals	Governance policies, processes and procedures (GV.PO-P)
Stage 1-2: Establish enterprise privacy risk management framework	Business environment (ID.BE-P)
Stage 1-3: Realize the benefits of privacy risk management	Business environment (ID.BE-P) Data protection policies, processes and procedures (PR.PO-P9) Communication policies, processes and procedures (CM.PO-P)
Stage 2: Conduct privacy risk management activities Stage 2-1: Define privacy risk assessment framework	Risk management strategy (GV.RM-P) Risk assessment (ID.RA-P)
Stage 2.2: Conduct privack risk assessments Stage 2-2-1: Vendor/third-party risk assessments Stage 2-2-2: Data breach readiness assessments	Data processing ecosystem risk management (ID.DE-P) Data protection policies, processes and procedures (PR.PO-P7, PR.PO-P8)
Stage 3: Implement risk response Stage 3-1: Establish response procedures for privacy risk	Data protection policies, processes and procedures (PR.PO-P10)
Stage 3-2: Response to privacy risk	Data protection policies, processes and procedures (PR.PO-P7)
Stage 3-3: Evaluate privacy risk response	Monitoring and review (GV.MT-P)

Figure 8—Mapping to ISO/IEC 27701

Privacy Risk Management Framework	ISO/IEC 27701
Stage 1: Establish privacy governance	5.4 Planning 6.3.1.5 Information security in project management
Stage 1-1: Define privacy governance goals	5.4 Planning 6.2 Information security policies
Stage 1-2: Establish enterprise privacy risk management framework	5.2 Context of the organization 5.3 Leadership
Stage 1-3: Realize the benefits of privacy risk management	5.5.1 Resources 6.4 Human resource security 6.3.1 Internal organization 5.5.4 Communication
Stage 2: Conduct privacy risk management activities Stage 2-1: Define privacy risk assessment framework	5.4.1.2 Information security risk assessment (planning) 5.4.1.3 Information security risk treatment (planning) 5.6.2 Information security risk assessment (operation) 5.6.3 Information security risk treatment (operation)
Stage 2-2: Conduct privacy risk assessments Stage 2-2-1: Vendor/third-party risk assessments	6.12 Supplier relationships 8.2.1 Customer agreement (processors) 8.5.6 Disclosure of subcontractors used to process personally identifiable information (PII) (processors) 8.5.7 Engagement of a subcontractor to process PII 8.5.8 Change of subcontractor to process PII
Stage 2-2-2: Data breach readiness assessments	6.13 Information security incident management 7.3.9 Handling requests (controllers)
Stage 3: Implement risk response Stage 3-1: Establish response procedures for privacy risk	6.9.4 Logging and monitoring
Stage 3-2: Response to privacy risk	6.14 Information security aspects of business continuity management
Stage 3-3: Evaluate privacy risk response	5.7 Performance evaluation 6.15 Compliance

- **French Data Protection Authority**—The Commission Nationale de l'informatique et des Libertés (CNIL) has proposed a methodology for privacy risk management.[14] By using a risk map (**figure 9**), the severity of a breach and its likelihood of occurrence can be determined. Severity is determined by the ease of identification and the potential prejudicial effects of the breach's impact. Likelihood is determined by the vulnerabilities of the supporting assets and the capabilities of the risk sources.

Stage 2-2: Conduct Privacy Risk Assessments

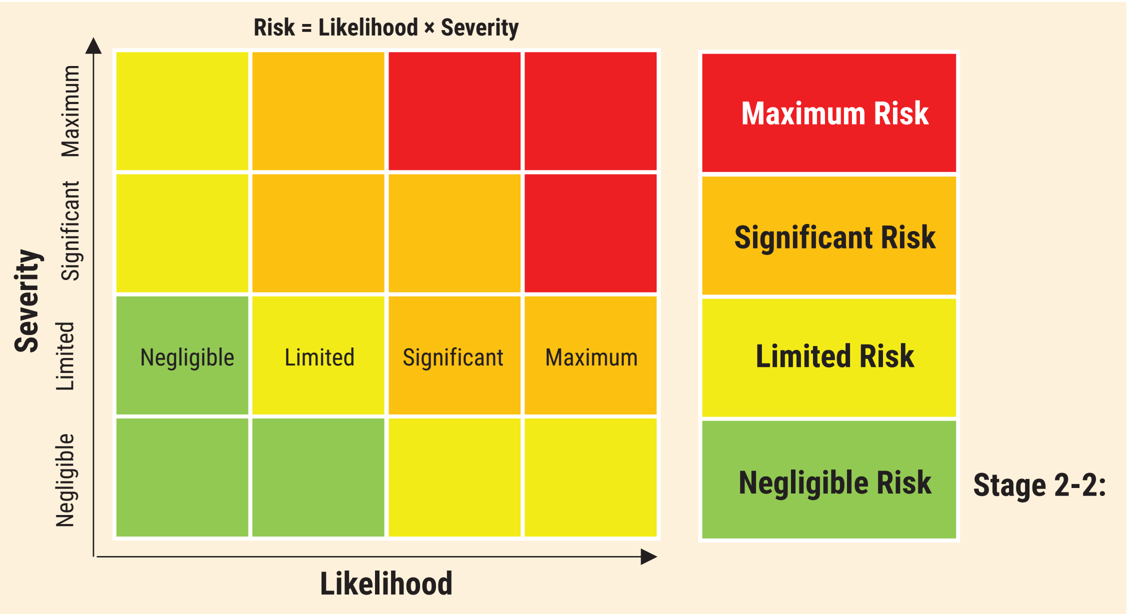
A privacy risk assessment is one of the critical procedures in privacy risk management. The aim is to assist enterprises in identifying the possible risk, vulnerabilities and threats during the data life cycle. There are many types of privacy risk assessments, which include vendor/third-party risk assessments and data breach readiness assessments (**figures 5** and **6**).

Stage 2-2-1: Vendor/Third-Party Risk Assessments

According to the IAPP survey, the most common type of risk assessment (performed by 63 percent of respondents, as shown in **figures 5** and **6**) is the vendor/third-party risk assessment.[15] The greater an enterprise's dependence on third parties or nth parties, the more complex a third-party risk assessment must be. Enterprises should consider the following factors related to threat, vulnerability and maturity:

- Determine whether the third party is aware of the core requirements of data protection.
- Check whether a DPIA has been conducted for the data processing operations performed by the third party; conduct a request for information (RFI)/request for quotation (RFQ), an on-site check, and regular audit and monitoring of the usage of software development kits (SDKs).

Figure 9—CNIL Risk Map



- Review whether the third party has certifications such as ISO/IEC 27001, Payment Card Industry Data Security Standard (PCI DSS) or other information security-related certifications.
- Review data sources, data types, data location, local regulatory requirements, data retention period, minimum safeguards and additional processing purposes, such as subcontracts to fourth or fifth parties.
- Review potential data combinations and additional uses that may impact the level of risk for individuals (e.g., artificial intelligence [AI], machine learning [ML], cloud computing technology) and whether the third-party possesses relevant qualifications.
- Disclose to customers any use of subcontractors to process personally identifiable information (PII).
- Cooperate only with third parties who can prove their compliance and provide adequate safeguards.
- In the case of general written authorization, inform customers of any intended changes concerning the addition or replacement of subcontractors.

Stage 2-2-2: Data Breach Readiness Assessments
To prepare for a data breach, assess the following:

- Level of risk of a data breach:
  - Considering the nature, scope, context and processing purpose of an incident, evaluate the risk associated with an independent event. If it affects large-scale data subjects or has a greater impact on specific individuals, the risk is high.
- Likelihood and severity of a personal data breach:
  - Type and nature of personal data involved, particularly special categories of personal data
  - Circumstances of a personal data breach
  - Whether appropriate technical safeguards have been applied (e.g., encryption, pseudonymization)
  - Whether the data subject will be directly or indirectly affected
  - Possibility that pseudonymization can be restored or that confidentiality fails
  - Possibility that personal data can be maliciously used
  - Possibility of substantial damage on a physical level
  - Nonsubstantial damage to the data subject

Several entities provide methodologies for data breach readiness assessments, including the following:

- **European Union Agency for Cybersecurity (ENISA)**—ENISA's methodology for assessing the severity of personal data breaches can be applied to identify and mitigate risk.[16] The criteria used to analyze the severity of the breach (SE) are data processing context (DPC), ease of identification (EI) and circumstances of the breach (CB), plus other factors that influence the overall scale of the breach: SE = DPC◊EI + CB
- **Spanish Data Protection Agency**—The Agencia Espanňola Protección Datos (AEPD) has established a set of criteria to assess risk based on the following factors: category or critical level; nature, sensitivity and categories of personal data affected; legible/illegible data; volume of personal data; ease of identifying individuals; severity of the consequences for individuals; individuals with special characteristics; number of individuals affected; data controllers with special characteristics (the entity itself); profile of the user affected; number and classification of the systems affected; impact; and legal and regulatory requirements.[17]

Stage 3: Implement Risk Response

Implementing the privacy risk response is the last stage of implementing a privacy risk management framework. In this phase the enterprise shall establish response procedures for privacy risk, take appropriate responses to the identified privacy risk and evaluate the privacy risk response. In this stage, the enterprise could do the tasks listed in **figure 10**.

Stage 3-1: Establish Response Procedures for Privacy Risk

After identifying privacy risk factors, enterprises should establish risk response procedures, taking into consideration the following aspects:

- Privacy policy
- Information security architecture
- Human resources (HR) controls
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operational security
- Communication security
- Systems acquisition
- Development and maintenance
- Third-party risk management (TPRM)
- Information security incident management
- Information security aspects of business continuity management (BCM)

Stage 3-2: Response to Privacy Risk

After identifying privacy risk, enterprises should take the appropriate action:

- **Mitigate risk**—Adopt the appropriate technical or administrative approaches in systems, products or services to minimize risk until an acceptable risk tolerance level is reached. Technical approaches include obfuscation technology, data minimization technology, security technology and privacy engineering technology. New technologies on the horizon include zero knowledge proofs, homomorphic encryption, secure multiparty computation, differential privacy, edge computing and local processing, device-level machine learning, identity management, small data, synthetic data sets, and generative adversarial networks.[18]
- **Transfer risk**—Sign contracts with the other enterprises involved.
- **Share risk**—Implement privacy notice and consent mechanisms as a means of sharing risk with individuals.

Stage 3-3: Evaluate Privacy Risk Response

Evaluation of the enterprise's privacy risk response should be ongoing to control, manage and report risk related to privacy risk management practices.

Figure 10—Creating and Implementing a Privacy Risk Management Framework—Stage 3: Implement Risk Response

Stage 3-1 Establish Response Procedures for Privacy Risk	**Stage 3-2** Response to Privacy Risk	**Stage 3-3** Evaluate Privacy Risk Response

At the same time, the enterprise should designate a specific person who is responsible for monitoring the privacy risk response, based on the enterprise's privacy risk governance goal. Monitoring ensures that implementation of the privacy plan is consistent with the enterprise's current privacy policies and standards. In addition, evaluation of the privacy risk response ensures achievement of the enterprise's privacy purpose by detecting failures early and obtaining feedback for improvement. When enterprises evaluate their privacy risk response, they should consider three indicators:

- **Compliance**—Can the enterprise ensure necessary policies and controls are in place for compliance during the collection, use and retention of personal data?
- **Regulation**—Does the response meet the requirements of applicable laws and regulations, which are constantly changing?
- **Environment**—Is there a risk of physical harm, programmatic concerns or insider threats?

> “ENTERPRISES SHOULD CARRY OUT INCIDENT RESPONSE REVIEWS OR POST-INCIDENT EVALUATIONS AFTER A SECURITY INCIDENT OCCURS.”

In particular, enterprises should carry out incident response reviews or post-incident evaluations after a security incident occurs. This includes reviewing configurations of personnel and resources and evaluating control approaches such as time and procedures.

Privacy Risk Management in Practice

Two real-life examples are provided here. The first focuses on performing a qualitative risk assessment based on an existing methodology. The second deals with one of the hottest privacy issues—employee tracking and monitoring—and how to implement privacy risk management in this scenario.

Example 1: Data Breach Risk Assessment Using the ENISA Methodology

In this example, two types of HR-related data breaches have occurred:

- **Case 1**—A file available on a shared drive containing more than 500 employees' names and dates of birth is accessed by nonauthorized employees.
- **Case 2**—An external contractor mails the monthly pay slips of eight employees to unauthorized recipients.

By applying the ENISA model,[19] the severity of the personal data breaches can be assessed.
For the first case:

- **DPC**—The names and dates of birth are simple data, so DPC = 1.
- **EI**—Because both the full name and the date of birth may be disclosed to others, there are two identifiers that can single out the individual, so EI = 1 (maximum).
- **CB**—The circumstance is loss of confidentiality. Nonauthorized employees can access the data, which means that the data can be disclosed to a number of known recipients, so CB = +0.25.

Therefore, SE = 1x1 + 0.25 = 1.25.

For the second case:

- **DPC**—The information on the pay slips is financial data, in particular, the kind of data that comes from a bank and concerns the account balances of clients for the last month, so DPC = 3.
- **EI**—The combination of information on the pay slips, such as full name and Social Security number, makes it easy to identify the individual, so EI = 1 (maximum).
- **CB**—Although the circumstance is the same as in the first case, the personal data have been sent to unauthorized recipients, which increases the impact of the breach because of the unknown number of recipients, so CB = +0.5 (higher than in the first case).

Therefore, SE = 3x1 + 0.5 = 3.5.

By conducting this type of qualitative assessment, an enterprise can evaluate the severity of breaches, which can help it prioritize its resources and influence privacy-related decision making.

Example 2: Employee Tracking and Monitoring
Few data controllers are likely to collect more personal data about individuals than their employers. So employee tracking and monitoring tools, such as those listed here, can impose a high privacy risk in the workplace:

- **Bring your own device (BYOD)**—Employees are permitted to use their own personal devices (e.g., smartphones, tablets) for communicating in the workplace. This results in a data protection risk because, outside the workplace, employees' mobile devices might be lost or misused; inside the workplace, the employer has access to personal data from employees' personal devices.
- **Data loss prevention (DLP)**—DLP tools inevitably involve processing the personal data of employees and other third parties because they operate on networks and systems used by employees, such as the email exchange server, which can contain personal information even if employees are not allowed to use it for personal activities.
- **Closed-circuit television (CCTV)**—CCTV is used to monitor the workplace for security purposes.
- **Email monitoring**—During an internal investigation, the employer may review employees' emails.
- **Global Positioning System (GPS) tracking**—GPS tracking devices may be installed in company cars.

Stage 1: Establish Privacy Governance
Before deciding whether to apply these monitoring tools, the enterprise should judge whether their use is based on data subject consent or legitimate interests. At the same time, the enterprise should establish appropriate policies (such as BYOD policies) and clearly explain to employees the purpose of collecting their personal data and the enterprise's responsibilities when doing so. For example, when deciding to apply DLP tools, the enterprise should strengthen the protection of its IT infrastructure and confidential business information through internal and external strategies.

Stage 2: Conduct Privacy Risk Management Activities
The enterprise should carry out a DPIA, LIA or balancing test on the employee monitoring activities to determine necessity, legitimacy, proportionality and transparency.

- **Necessity**—Whether monitoring is necessary to the processing purpose and meets data minimization requirements
- **Legitimacy**—Whether monitoring (e.g., large-scale video surveillance or the systematic monitoring of public areas) meets legitimate interests, such as protecting the IT infrastructure of maintaining the safety of public areas
- **Proportionality**—Whether monitoring is proportionate to the issue the enterprise is encountering (e.g., remote control, facial recognition and voice recording may not be necessary)
- **Transparency**—Whether the existence and type of surveillance measures have been communicated to employees

Stage 3: Implement Risk Response

- Be clear about where the processed data are stored and what measures must be taken to keep them secure.
- Ensure that the transfer of data from employees' personal devices to the enterprise's servers is secure to avoid any interceptions.
- Consider how to manage personal data held on personal devices once an employee leaves the company or if a device is stolen or lost. Mobile device management software can be used to locate devices and remove data on demand.
- Obtain prior authorization when required. For instance, in most countries, enterprises installing CCTV should obtain advance certification from supervisory authorities, in accordance with local regulations.
- After monitoring has been implemented, make the following determinations with regard to personal data: whether there is a legal basis for retaining data; whether the data are stored safely; whether the data retention period is defined; whether data subjects can exercise their rights, including the right to complain; whether the data will be anonymously processed or destroyed.

Conclusions

Privacy is not just a compliance issue anymore. It is about managing consumer trust and safeguarding personal data during the data life cycle. Creating and implementing a privacy risk management framework is the critical step an enterprise should take to build trust and protect data.

> “PRIVACY...IS ABOUT MANAGING CONSUMER TRUST AND SAFEGUARDING PERSONAL DATA DURING THE DATA LIFE CYCLE.”

Endnotes

[1] International Association of Privacy Professionals, “2020 Global Legislative Predictions,” *https://iapp.org/media/pdf/resource_center/global_legislative_predictions_2020.pdf*

[2] RSA Conference 2020, “NIST Privacy Framework IRL: Use Cases From the Field,” *https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/17967/2020_USA20_PRV-W01_01_NIST%20Privacy%20Framework%20IRL%20Use%20Cases%20from%20the%20Field.pdf*

[3] Intersoft Consulting, Art. 4: Definition, EU General Data Protection Regulation (GDPR), Belgium, 2018, *https://gdpr-info.eu/art-4-gdpr/*

[4] ISACA®, *COBIT® 5: Enabling Information*, USA, 2013, *https://www.isaca.org/bookstore/cobit-5/cb5ei*

[5] ISACA, *Rethinking Data Governance and Management: A Practical Approach for Data-Driven Enterprise*, USA, 2020, *https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whprdg*

[6] ISACA, COBIT® 2019, USA, 2018, *https://www.isaca.org/resources/cobit*

[7] National Institute of Standards and Technology (NIST), NIST Privacy Framework Core Version 1.0, USA, 16 January 2020, *https://www.nist.gov/privacy-framework*

[8] *Ibid*.

[9] International Association of Privacy Professionals, “Measuring Privacy Operations 2019—Cookies, Local vs. Global Compliance, DSARs and More,” *https://iapp.org/media/pdf/resource_center/trustarc_survey_iapp.pdf*

[10] International Association of Privacy Professionals, “Privacy Program Management—Tools for Managing Privacy Within Your Organization,” *https://iapp.org/store/books/a191P0000035CgQQAU/*

[11] *Ibid*.

[12] *Op cit* National Institute of Standards and Technology

[13] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27701 *Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines*, 2019, *https://www.iso.org/standard/71670.html*

[14] Commission Nationale de l’informatique et des Libertés (CNIL), “Methodology for Privacy Risk Management: How to Implement the Data Protection Act,” *https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf*

[15] *Op cit* International Association of Privacy Professionals, “Measuring Privacy Operations 2019”

[16] European Union Agency for Cybersecurity (ENISA), “ENISA Recommendations for a Methodology of the Assessment of Severity of Personal Data Breaches,” November 2013, *www.e-szbi.pl/files/Data-breach-severity-methodology.pdf*

[17] Agencia Espanňola Protección Datos (AEPD), “Guide on Personal Data Breach Management and Notification,” September 2019, *https://www.aepd.es/sites/default/files/2019-09/Guide-on-personal-data-breach.pdf*

[18] Polonetsky, J.; E. Renieris; *Privacy 2020: 10 Privacy Risk and 10 Privacy Enhancing Technologies to Watch in the Next Decade*, Future of Privacy Forum, USA, January 2020, *https://fpf.org/wp-content/uploads/2020/01/FPF_Privacy2020_WhitePaper.pdf*

[19] *Op cit* ENISA