Aligning COSO and Privacy Frameworks to Manage Privacy in a Post-GDPR World

There is one constant in the data privacy landscape: change. The EU General Data Protection Regulation (GDPR) was adopted in 2016 to protect the personal data of EU citizens and harmonize data privacy laws across EU member states. Since then, data privacy has become a growing concern for boards of directors (BoDs). While global organizations, in addition to healthcare and financial institutions, had some prior experience with privacy regulations, compliance with the growing number of comprehensive privacy laws, e.g., GDPR, Brazil's data protection regulation (Lei Geral de Proteção de Dados [LGPD]) and new US state laws such as the California Consumer Privacy Act (CCPA) are new and unknown business challenges for many organizations. This is a rapidly growing issue—a number of US states proposed new privacy laws in 2019, and countries around the globe have enacted many other new regulations over the last three years. Simply put, keeping up with privacy compliance is now a never-ending task.[1]

Many organizations are actively looking for standardization in evaluating privacy risk and ensuring that the controls in place align with enterprise risk management objectives. Compliance can be streamlined by aligning new privacy frameworks with the Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2013 *Internal Control—Integrated Framework*, a well-established, widely used framework.

There are several privacy standards and frameworks that can underpin a privacy program. Some governments and national standards bodies have developed standards to facilitate compliance with privacy and data protection requirements, such as British Standard 10012, which establishes a path toward certification to demonstrate compliance with data protection regulations like GDPR.[2] Others have outlined frameworks for ensuring that appropriate privacy protections are in place.

Donel Martinez, CISA, CAMS, CSF Practitioner
Is a director in the risk advisory practice of Focal Point Data Risk, specializing in audit and compliance and their application to areas such as cybersecurity and privacy. Martinez has led many large-scale compliance engagements covering areas such as IT, information security, the US Sarbanes-Oxley Act of 2002 (SOX) and data privacy. He has extensive knowledge of regulatory standards and frameworks, including SOX, the US Health Insurance Portability and Accountability Act (HIPAA), US National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), ISO 27001, the US Bank Secrecy Act (BSA) and US-state-specific standards.

Joshua Marks, JD, CIPP/US
Is a manager with Focal Point Data Risk's national data privacy practice. Marks supports Focal Point's clients with his wide-ranging data privacy laws and regulations experience. He has aided governmental organizations, multinational corporations and regional enterprises in operational compliance efforts to meet the data privacy requirements of laws such as the EU General Data Protection Regulation and the US State of California's Consumer Privacy Act. Prior to joining Focal Point, Marks was a civil litigation attorney and practiced for nearly 10 years defending corporations in state and federal court litigation. He is also a recognized industry thought leader and provides guidance to other legal professionals on data privacy and security issues through his involvement with nonprofit bar associations.

For instance, the Asia-Pacific Economic Cooperation (APEC) created the APEC Privacy Framework, a principles-based framework for the 21 member countries of APEC's regional economic forum, to encourage the development of appropriate privacy protections in the Asia-Pacific region.[3] The APEC Privacy Framework serves as a basis for the APEC Cross-Border Privacy Rules System, which establishes an accountability mechanism for organizations to certify their data privacy practices.[4]

In addition, the US National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), whose respective cybersecurity frameworks are used by many organizations, both developed new privacy frameworks/standards. The NIST Privacy Framework was released on 16 January 2020.[5] Additionally, the ISO/IEC 27701 standard, published in 2019, builds on the privacy framework described in ISO 29100, mapping specific privacy-related controls to the framework.[6] Both have already been utilized by organizations seeking a solid foundation for their privacy program.

The widely used COSO framework describes five key components of internal control that must exist to achieve an entity's mission: a control environment, risk assessments, control activities, information and communication, and monitoring activities.[7] Further, the COSO framework defines 17 principles aligned with these five key components (**figure 1**). To align with COSO, a privacy framework should:

- Define a privacy control environment
- Establish a risk assessment for privacy
- Document applicable privacy control activities
- Effectively communicate privacy requirements
- Establish processes for monitoring and maintaining compliance

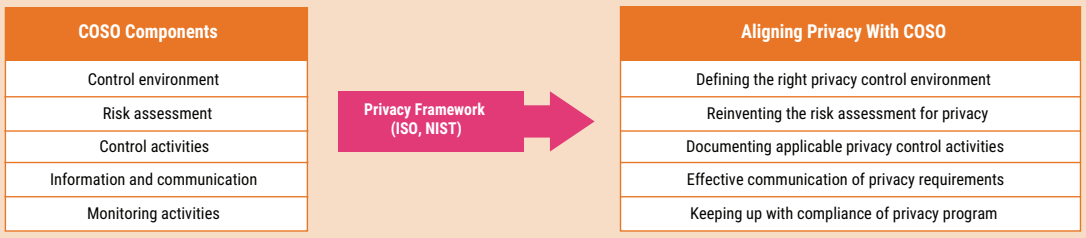
> "THE CONTROLS NEED TO MEET THE OBJECTIVES OF THE ORGANIZATION, BUT THEY ALSO NEED TO BE REALISTIC, RECOGNIZING THE CAPABILITIES OF THE TEAM AND AVAILABLE RESOURCES."

Defining the Right Privacy Control Environment

Per the COSO framework, the control environment is the set of standards, processes and structures that provides the basis for carrying out internal control across the organization. Designing the right control environment for an organization is a balancing act. The controls need to meet the objectives of the organization, but they also need to be realistic, recognizing the capabilities of the team and available resources. While each control environment is unique, COSO establishes five guiding principles:

1. Demonstrating commitment to integrity and ethical values
2. Exercising oversight responsibility
3. Establishing structure, authority and responsibility
4. Demonstrating commitment to competence
5. Enforcing accountability

Figure 1—Aligning a Privacy Framework With COSO



A privacy program may meet these principles by ensuring board involvement, authority and responsibility, and an appropriate team.

Board Involvement
First, the organization must demonstrate a commitment to integrity and ethical value and involve the BoD. As with all significant enterprise risk, the board has ultimate accountability for the strategies in place to protect the organization. As such, the board should have regular conversations with the privacy officer or person responsible for maintaining the privacy program.

The Establishment of Authority and Responsibility
The organization must establish, with board oversight, a formal charter for the privacy program. This charter can:

- Define the privacy team and a privacy committee, if applicable
- Define roles and responsibilities for oversight and alignment with strategy and objectives
- Set the tone for the introduction, design or enhancement of privacy controls and privacy compliance management
- Identify the responsibilities and the relationship of the chief information security officer (CISO) and security functions with the privacy function
- Provide the process for the review and approval of privacy-related policies and procedures

Those establishing this charter should also involve human resources (HR) to build a strong sanction program related to privacy concerns and issues. Embedding privacy throughout the organization is a key component. For instance, privacy concerns can be addressed by taking privacy into account when creating any engineering process (i.e., privacy by design) and by appointing privacy liaisons across the organization.

Building and Maintaining a Team
The team responsible for maintaining privacy operations must have the skills and capabilities outlined in the privacy charter. This list of skills will likely be long and will probably have to evolve as technology advances. Competencies outside the privacy team also need to be evaluated. Marketing, IT operations and HR need to protect the data in their care as well. An adequate training program must exist and should include different courses for different responsibilities, such as training for users who need to action privacy (e.g., software development, HR, marketing personnel), and broader awareness of the privacy program and privacy requirements for larger audiences.

> "THE TEAM RESPONSIBLE FOR MAINTAINING PRIVACY OPERATIONS MUST HAVE THE SKILLS AND CAPABILITIES OUTLINED IN THE PRIVACY CHARTER."

Reinventing the Risk Assessment for Privacy

Risk assessment is a "dynamic and iterative process for identifying and assessing risks to the achievement of objectives"[8] across the organization. Those risk factors are considered relative to established risk tolerances. Therefore, a risk assessment is the basis for determination of how to manage risk across the organization. COSO identifies four principles supporting this component:[9]

1. Specifying suitable objectives
2. Identifying and analyzing risk
3. Assessing fraud risk
4. Identifying and analyzing significant change

Performing a risk assessment that addresses privacy concerns and aligns with the COSO framework requires the development of a methodology applicable to the environment and the unique challenges of privacy risk.

According to NIST, while managing cybersecurity risk is necessary to address privacy risk, it is not sufficient, as privacy risk may arise beyond the scope of cybersecurity concerns.[10] For instance, while cybersecurity risk factors are associated with the loss of confidentiality, integrity and availability of

> BY PERFORMING AN INFORMATION MAPPING EXERCISE THAT IDENTIFIES THE LIFE CYCLE OF PII THROUGHOUT THE ORGANIZATION…PRIVACY LEADERS CAN BETTER INFORM MANAGEMENT OF THE PRIVACY RISK RELATED TO THAT PII.

information, privacy risk factors are associated with the unintended consequences of data processing. In other words, a privacy risk is the "likelihood that individuals will experience problems resulting from data processing, and the impact should they occur."[11] NIST further defines privacy risk in the NIST Internal Report (IR) 8062, "An Introduction to Privacy Engineering and Risk Management in Federal Systems,"[12] Section 3.2, and the Privacy Risk Assessment Methodology (PRAM), which was created as an application of the NIST IR 8062 risk model to help organizations analyze, assess and prioritize privacy risk. It identifies the following four impact factors of privacy risk:[13]

1. Noncompliance costs such as regulatory fines, litigation costs, etc.
2. Direct business costs such as revenue or performance loss from customer abandonment or avoidance
3. Reputational costs such as brand damage, loss of customer trust, etc.
4. Internal culture costs such as impact on capabilities

It may also be helpful to add consumer impact as a fifth factor that considers the level of potential financial loss consumers would experience.

Similarly, NIST defines some factors organizations may use to assess the likelihood of risk factors such as customer demographics and information available about privacy problems in similar scenarios.[14] However, every organization may consider **figure 2** in making this assessment.

All these risk factors should be carefully considered and clearly communicated to executive leadership and the board so they can determine easily if their privacy risk aligns with the risk appetite of the organization.

Documenting Applicable Control Activities

The COSO framework describes control activities as the "actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out."[15] Control activities are performed at "all levels of the entity, at various stages

Figure 2—Likelihood Risk Factors

Business Profile	Regulatory Change	Regulatory Environment
• Number of records processed • Number of new/revised processing methods • Outsourcing • Sophisticated environment	• Complexity of requirements • Changes in last 24 months • Availability of guides relating to non-substantive requirements	• Emerging area of focus • Government examinations • Litigation and enforcement activities • Consumer advocacy groups, legislators and media

within business processes, and over the technology environment."[16] Three principles should be present to meet this COSO framework component:[17]

1. Selecting and developing control activities
2. Selecting and developing general controls over technology
3. Deploying through policies and procedures

Selecting and developing applicable control activities should be connected to the risk assessment, identifying control activities for key or critical personally identifiable information (PII). Because all PII is in scope, prioritization is very important. Control activities should be feasible to accomplish with the assigned resources.

Performing privacy impact assessments (PIAs), which include the evaluation and identification of privacy risk associated with an organizational process, may help identify control activities across the organization.[18, 19] Additionally, the Control-P Function of the NIST Privacy Framework Core suggests minimum control activities in an effective control environment, such as procedures for authorizing data processing.[20] Different functions and skill sets are necessary to design, maintain and test the different privacy controls (**figure 3**).

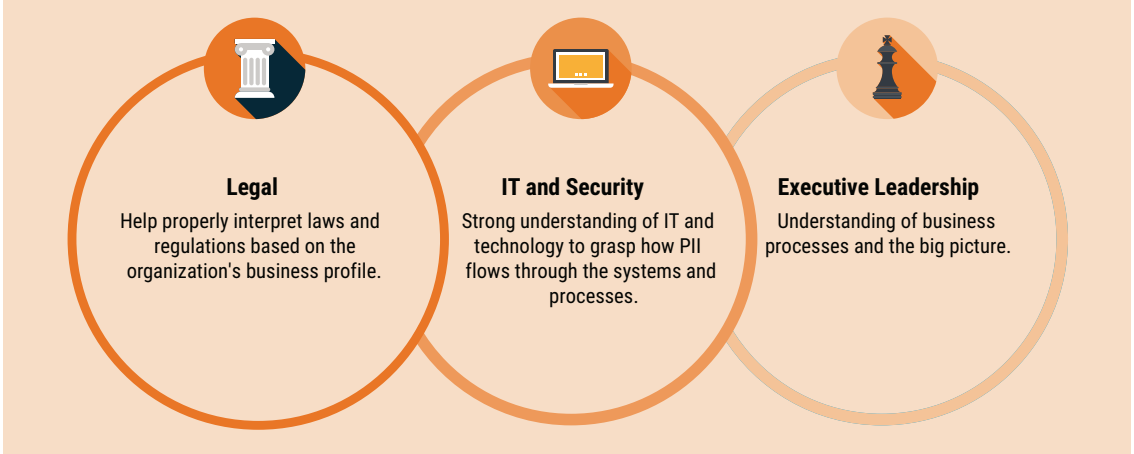
By performing an information mapping exercise that identifies the life cycle of PII throughout the organization, including how it is processed, the purposes of its use, where it is retained and how it is shared, privacy leaders can better inform management of the privacy risk related to that PII.

In addition, organizations must evaluate their mix of control activities, such as system access, system configuration, review controls and authorization, while considering several attributes for each control, such as:[21, 22]

- The category of the control (e.g., key performance indicator [KPI]/key risk indicator [KRI], third-party oversight)
- Whether the control is preventive or detective
- Whether the control is a system/automated control or a manual control
- Whether the control is maintained internally or externally by a third party
- The frequency of the control execution

All controls should be rated, and the first rating may be based on the strength of these attributes. For example, an automated control may be more effective than a manual control, and a preventive control may be more effective than a detective control. Control activities must also be deployed through policies and procedures, which should be implemented to support management's directives. They should establish responsibility and accountability for the execution of privacy controls.

Figure 3—Business Functions That Help Support Privacy



Enjoying this article?

- Read *Implementing the General Data Protection Regulation. https://next.isaca.org/bookstore/cobit-5/wgdpr*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

To illustrate with an example, many privacy regulations such as GDPR,[23] Brazil's LGPD[24] and the CCPA[25] provide individuals certain rights, such as access to their own data/PII possessed by an organization. These rights must be granted upon a proper request made by the individual. To comply with requests, individual rights fulfillment processes must be in place to address, for instance, requests by the individual to access or delete PII handled by the organization. Inevitably, policies, procedures and practices must be established regarding this requirement. An organization with a less complex PII landscape may be capable of fully automating the fulfillment process, thereby establishing an automated control over the fulfillment. Other organizations may use manual controls, established through detailed procedures and tracking of fulfillment. Those organizations might include an oversight control function to review fulfillment prior to completion.

> "AS A PREVENTIVE CONTROL, ALL ORGANIZATIONS SHOULD INCLUDE PRIVACY TRAINING FOR EMPLOYEES WHO HANDLE PII SO THEY CAN RECOGNIZE THE RIGHTS THAT APPLY AND DIRECT DATA SUBJECTS TO THE APPROPRIATE CHANNELS FOR REQUESTS."

In addition, compliance is not just a legal, compliance or privacy team function. As a preventive control, all organizations should include privacy training for employees who handle PII so they can recognize the rights that apply and direct data subjects to the appropriate channels for requests.

Meeting Effective Communication Requirements for Privacy

The COSO framework identifies "information and communication" as a core component of internal control. Certainly, quality data to inform control activities is necessary to effectively execute internal control responsibilities. Additionally, communication within and outside the organization through a continuous and iterative process of sharing information is just as critical to internal control.[26] Communication within the organization may include the dissemination of the objectives and responsibilities for internal control. Communication outside the organization may establish or meet the requirements and expectations of external parties. COSO defines three principles related to this component:[27]

1. Obtaining and using relevant and quality information
2. Communicating internally
3. Communicating externally

Every stakeholder involved in managing privacy risk must consider the quality and effectiveness of communications. The board and executive leadership set the tone and must build a culture that prioritizes clear and direct communication about privacy risk and obligations. In addition, communication with external parties, including regulatory organizations, should be clear and consistent. For instance, the Communicate-P function defined in the NIST Privacy Framework recommends developing and implementing "appropriate activities to provide organizations and individuals with a reliable understanding about how data is processed and the associated privacy risks."[28] As the NIST Privacy Framework describes, this might include establishing formal policies and training to ensure that impacted individuals and organizations are notified in the event of a privacy breach. It may also include developing transparent policies to communicate data processing purposes and implementing mechanisms for obtaining feedback from individuals about data processing risk.

Managing the Compliance of the Privacy Program

The "monitoring activities" component of the COSO framework suggests establishing evaluations to ensure that each of the COSO framework components and principles are present and functioning.[29] Business processes may contain

> EVERY STAKEHOLDER INVOLVED IN MANAGING PRIVACY RISK MUST CONSIDER THE QUALITY AND EFFECTIVENESS OF COMMUNICATIONS.

ongoing evaluations at all levels in the organization, ensuring consistent application of the framework. Moreover, periodic evaluations may be conducted with varying scope and frequency, depending on the organization's risk profile, to focus on specific concerns or other management considerations. Findings may be evaluated against standard-setting bodies or regulations, while deficiencies should be communicated to organization leadership.[30] The two COSO principles related to this component include conducting ongoing evaluations and evaluating and communicating deficiencies.

Ongoing monitoring (the second line of defense) and independent evaluations (the third line of defense) should be considered in the development and maintenance of any privacy program to evaluate its effectiveness and communicate its deficiencies. For instance, the NIST Privacy Framework Core describes, within the Monitoring and Review category of the Govern-P function, an ongoing review of the organization's privacy posture to inform management of privacy risk.[31] Subcategory GV.MT-P1 describes the reevaluation of privacy risk on an ongoing basis, including key factors such as the organization's business environment, legal obligations, risk tolerance and data processing functions.[32] An organization seeking to align its privacy program with the COSO framework may incorporate these elements in its control environment to ensure ongoing compliance.

Three Control Objectives

Within COSO, there are three central control objectives focused on operations, reporting and compliance. These three control objectives may be applied to privacy controls (**figure 4**).

Operations

The COSO framework defines operational objectives of internal control as pertaining to the effectiveness and efficiency of the entity's operations. These may include operational and financial performance goals and safeguarding assets against loss.[33] When it comes to managing privacy control operation objectives, an organization may consider both the type of PII and its use within the operations of the organization. PII may be involved in marketing processes, employment processes, consumer product fulfillment processes and many others throughout the organization. The applicable privacy controls that align with business operations in those varied areas may differ. However, the central objective of maintaining the privacy of PII throughout the organization's operations is overarching. Thus, the operations objective informs the selected controls.

Reporting

COSO reporting objectives typically pertain to internal and external financial and nonfinancial reporting,

Figure 4—Examples of Privacy Control Objectives

which may encompass reliability, timeliness, transparency or other terms set forth by regulators.[34] In the world of privacy compliance, the type, transparency and timing of reporting are critical. When establishing reporting processes, determining who relies on each report type (e.g., breach notifications, privacy KRIs) and tailoring the reports to that audience are good starting points. The following types of reports are critical to the success of many privacy programs: incidents/breaches, data subject rights fulfillment, third-party risk management metrics and privacy-related KRIs.

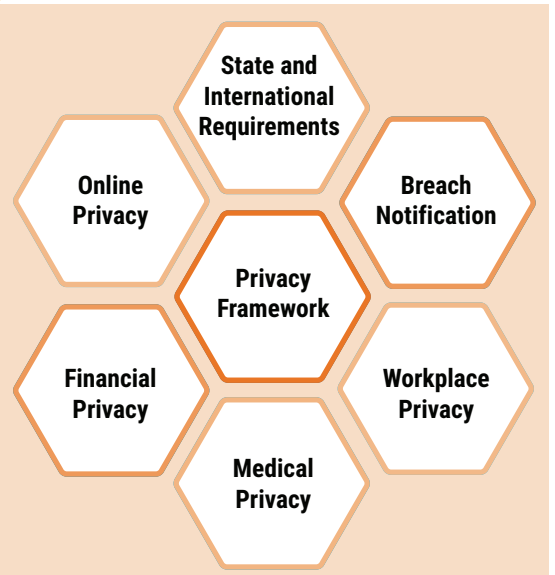
To remain compliant with a number of privacy regulations, the timing of these reports is a critical factor. For example, GDPR requires that organizations provide notice of a breach in 72 hours.[35] In addition, regular internal reporting to executives and boards on the effectiveness of the privacy program is key to maintaining investments in privacy and ensuring that the right resources are in place to reduce privacy risk.

> "WHEN IMPLEMENTING A PRIVACY FRAMEWORK, IT IS IMPORTANT TO CONSIDER HOW IT ALIGNS WITH ALL APPLICABLE LAWS AND REGULATIONS AND WHETHER IT IS FLEXIBLE ENOUGH TO ACCOMMODATE FUTURE REGULATORY REQUIREMENTS."

Compliance

Compliance objectives pertain to an organization's adherence to laws and regulations.[36] When implementing a privacy framework, it is important to consider how it aligns with all applicable laws and regulations and whether it is flexible enough to accommodate future regulatory requirements (**figure 5**). Although requirements vary by regulation, strong privacy controls applied consistently across an organization help decrease the effort needed to meet new requirements. Many fundamental privacy concepts such as privacy notices or individual rights to PII are common to most new privacy regulations. Identifying these universal concepts and utilizing privacy frameworks to implement them aids in the development of a control environment that is compliant, and effectively manages privacy risk.

Figure 5—Compliance Concerns Addressed by a Framework



Hierarchical Application

For a privacy framework to align with COSO, it must apply to the whole organization—from entity-level controls that set the tone at the top of the organization to controls specific to certain business functions. For example, NIST Framework Core subcategory GV.PO-P1 states, "Organizational privacy values and policies … are established and communicated."[37] This would likely be defined as an entity-level control. In comparison, while the basis of subcategory CT.DP-P2, "Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization)," might apply across the organization, execution procedures would need to be tailored to each business function.[38] Mapping a framework across an organization is not an easy step. It requires the organization to determine which controls should be applied at the entity level and which should be tailored to specific business processes.

> WITHOUT A PRIVACY FRAMEWORK IN PLACE, IT IS NEARLY IMPOSSIBLE FOR AN ORGANIZATION TO KEEP PACE WITH CHANGING DATA PROTECTION REGULATIONS.

The Benefits of Aligning Privacy With COSO

Without a privacy framework in place, it is nearly impossible for an organization to keep pace with changing data protection regulations, putting the organization at great risk. Using a framework that aligns with a widely adopted standard such as COSO provides a number of benefits:

- **Streamlined efforts**—Aligning privacy controls with COSO greatly reduces the burden on audit, operations and implementation teams, requiring fewer audits and streamlining remediation efforts
- **Cost and time savings**—Addressing privacy compliance *ad hoc* is a costly experiment. By using a framework, organizations can apply privacy controls across regulations, minimizing the number of resources needed to manage compliance, reducing compliance costs and saving significant time. In addition, a framework helps reduce the risk of fines and penalties for noncompliance through a common structure and standardization.
- **Sustainable compliance**—Implementing a privacy framework makes it possible for the organization to scale its privacy program with organizational change, new technologies and shifting regulations.

While choosing and customizing a framework does require a good amount of effort up front, when implemented properly, it can save an organization time, resources and budget for years to come.

Endnotes

1 Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control—Integrated Framework*, Executive Summary, 2013, *https://www.coso.org/Pages/ic.aspx*

2 British Standards Institution, British Standard 10012, *Personal Information Management*, 2017, *https://www.bsigroup.com/en-GB/BS-10012-Personal-information-management/Introduction-to-BS-10012/*

3 Asia-Pacific Economic Cooperation, *APEC Privacy Framework (2015)*, August 2017, *https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)*

4 Cross Border Privacy Rules System, "Policies, Rules and Guidelines," *http://cbprs.org/documents/*

5 National Institute of Standards and Technology, "NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management," USA, 16 January 2020, *https://www.nist.gov/privacy-framework/privacy-framework*

6 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), *Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management—Requirements and Guidelines*, August 2019, *https://www.iso.org/standard/71670.html*

7 *Op cit* Committee of Sponsoring Organizations of the Treadway Commission

8 *Ibid*.

9 *Ibid*.

10 *Op cit* National Institute of Standards and Technology

11 *Ibid*.

12 Brooks, S.; M. Garcia; N. Lefkovitz; S. Lightman; E. Nadeau; "An Introduction to Privacy Engineering and Risk Management in Federal Systems," National Institute of Standards and Technology (NIST) Internal Report (IR) 8062, USA, January 2017, *https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf*

13 National Institute of Standards and Technology, "Risk Assessment Tools," USA, 28 October 2018, *https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/browse/risk-assessment-tools*

14 *Op cit* National Institute of Standards and Technology, January 2020

15 *Op cit* Committee of Sponsoring Organizations of the Treadway Commission

16 *Ibid*.

17 *Ibid*.

18 *Op cit* National Institute of Standards and Technology, January 2020

19 *Op cit* National Institute of Standards and Technology, October 2018

20 *Op cit* National Institute of Standards and Technology, January 2020
21 *Ibid*.
22 *Op cit* Committee of Sponsoring Organizations of the Treadway Commission
23 European Parliament, "Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)," 2016
24 Lei No. 13.709, de 14 de Agosto de 2018, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] de 15.8.2018 (Braz.). Lei Geral de Proteção de Dados Pessoais, Art. 18, *http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm* (Unofficial English translation available at: *https://iapp.org/resources/article/brazils-general-data-protection-law-english-translation/)*
25 California Consumer Privacy Act, California Civil Code § 1798.100-125, USA, 2018
26 *Op cit* Committee of Sponsoring Organizations of the Treadway Commission
27 *Ibid*.
28 *Op cit* National Institute of Standards and Technology, January 2020
29 *Op cit* Committee of Sponsoring Organizations of the Treadway Commission
30 *Ibid*.
31 *Op cit* National Institute of Standards and Technology, January 2020
32 *Ibid*.
33 *Op cit* Committee of Sponsoring Organizations of the Treadway Commission
34 *Ibid*.
35 *Op cit* European Parliament
36 *Op cit* Committee of Sponsoring Organizations of the Treadway Commission
37 *Op cit* National Institute of Standards and Technology, January 2020
38 *Ibid*.