A Guide to Selecting and Adopting a Privacy Framework

COVID-19 imposed change on every aspect of life and business in 2020, but 2020 was also a significant year in the world of privacy protection for reasons beyond the pandemic. In 2020, enforcement of the EU General Data Protection Regulation (GDPR) was in full swing. The US State of California Consumer Privacy Act (CCPA) went into effect, and enforcement began. California’s Consumer Privacy Rights Act (CPRA)—called CCPA 2.0 by some—was also drafted and passed. Across the globe, 79 percent of organizations are managing compliance with two or more privacy regulations.¹ This inundation of privacy regulations has introduced a number of new challenges, including duplicative compliance efforts, conflicting or changing policies, increased operational costs, and disparate processes.

By taking a page from the cybersecurity playbook, privacy teams can adopt a privacy framework (or multiple frameworks) to streamline compliance efforts, build a unified privacy strategy, and establish or advance privacy programs. Teams must determine how to prepare an enterprise for framework adoption, how to select a framework that is the right fit and how to integrate it into the enterprise.

A Privacy Framework Primer

Before diving into the nuances of selecting and adopting a privacy framework, it is important to understand how a framework is defined and which privacy frameworks are available. A privacy framework is a comprehensive collection of processes that protect personal information and address privacy risk. The two key characteristics of a privacy framework are a clear structure and principles that are broad in nature, making them universally applicable and easy to adopt. Because of these features, frameworks can help enterprises of all sizes, in all industries and at all levels of maturity evaluate and monitor their privacy programs.

In the United States, privacy frameworks began to appear in the 1970s, with the debut of the Fair Information Practice Principles (FIPPs).² Some frameworks, such as the US National Institute of Standards and Technology (NIST) Privacy Framework, are merely a set of recommendations and are not enforced by any regulatory body. But regulations, principles, and standards such as GDPR, FIPPs or International Organization for Standardization (ISO) ISO 29100 can also be leveraged as frameworks. Some organizations have chosen to make GDPR more than just a regulatory requirement, using it as a guiding framework because of its robust privacy principles and specific requirements that establish strong data protection practices. Here the term “framework” will be used

Minaz Khan, CISA, CIPT

is a senior consultant in Focal Point’s cybersecurity and data privacy practice. Her experience includes conducting privacy and cybersecurity assessments, focusing on regulations such as the EU General Data Protection Regulation (GDPR) and the US Health Insurance Portability and Accountability Act (HIPAA), and specializing in frameworks created by the US National Institute of Standards and Technology (NIST) and the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). Previously, she worked as an information technology auditor for Boeing Distribution Services, where she conducted risk assessments, information system audits and US Sarbanes-Oxley Act (SOX) compliance testing.
broadly to also include standards and regulations that can be (and are) used to build, govern and maintain privacy programs. Some of the top privacy frameworks and regulations are shown in figure 1.

It is worth noting that some privacy frameworks, including the NIST Privacy Framework, ISO 27701 and ISO 29100, have been pushed into the spotlight by their cybersecurity counterparts: NIST Cybersecurity Framework (CSF), NIST Special Publication (SP) 800-53 and ISO 27001/27002. Because these cybersecurity frameworks are long-standing industry fixtures, many enterprises have been encouraged to adopt the complementary privacy frameworks.

Preparing for Framework Selection

Selecting a framework requires input from various perspectives and thorough preparation. An enterprise should not choose the NIST Privacy Framework simply because it is already following the NIST CSF. Similarly, an enterprise should not build its entire privacy program on GDPR because it has operations in the European Union. Instead, several key questions should be considered before selecting a framework (or frameworks).

Question 1: Who Should Be Involved?

Although a privacy framework will be used primarily by those focused on privacy efforts (e.g., privacy team, legal, compliance, risk management), it will impact many other parts of the enterprise. Conversely, frameworks and regulations followed by other parts of the business may influence which privacy framework is selected.

To properly evaluate the available frameworks, the right selection team must be created. Selection teams may vary by organizational size and structure, industry, and regulatory landscape. However, the following functions may have a stake in choosing a framework because they work directly or indirectly with personally identifiable information (PII).

- **Cybersecurity**—Cybersecurity and privacy functions should work together very closely. Cybersecurity may already be using a framework that has a privacy counterpart. In addition, cybersecurity may be able to offer insights into which data security recommendations are a good fit for the enterprise.

- **Information technology**—Leaders with knowledge of the systems that touch personal information are a critical part of this process. Chief information officers (CIOs) and chief

<table>
<thead>
<tr>
<th>Year</th>
<th>Framework, Standard, Regulation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1973</td>
<td>FIPPs</td>
<td>Establishes privacy principles within government</td>
</tr>
<tr>
<td>1974</td>
<td>US Privacy Act of 1974</td>
<td>Establishes Code of Fair Information Practice to govern personally identifiable information (PII)</td>
</tr>
<tr>
<td>2000</td>
<td>Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada)</td>
<td>Governs privacy in ecommerce</td>
</tr>
<tr>
<td>2005</td>
<td>Asia-Pacific Economic Cooperation (APEC) (Asia Pacific)</td>
<td>Addresses privacy in the Asia-Pacific region</td>
</tr>
<tr>
<td>2009</td>
<td>Generally Accepted Privacy Principles (GAPP)</td>
<td>Criteria for audits and compliance</td>
</tr>
<tr>
<td>2011</td>
<td>ISO 29100 Information technology—Security techniques—Privacy framework</td>
<td>Provides terminology, roles and principles for privacy</td>
</tr>
<tr>
<td>2012</td>
<td>US Consumer Privacy Bill of Rights</td>
<td>Regulates the processing of electronic personal data in the US</td>
</tr>
<tr>
<td>2016</td>
<td>EU GDPR</td>
<td>Harmonizes privacy across the European Union</td>
</tr>
<tr>
<td>2019</td>
<td>ISO 27701 Privacy Information Management</td>
<td>Provides Privacy Information Management Systems (PIMS) guidance</td>
</tr>
<tr>
<td>2020</td>
<td>US NIST Privacy Framework</td>
<td>Identifies and addresses privacy risk</td>
</tr>
<tr>
<td>2020</td>
<td>Association of International Certified Professional Accountants (AICPA) Privacy Management Framework</td>
<td>Addresses privacy obligations and risk while advancing the business</td>
</tr>
</tbody>
</table>
technology officers (CTOs) may be able to weigh in on how systems and IT controls will be affected by a framework.

- **Information security**—Information security leaders are dedicated to protecting the data that flow into and out of an enterprise and can offer critical insights into how personal information is handled and stored throughout the enterprise.

- **Legal**—Legal and privacy teams are often closely linked—sometimes they are one and the same. The legal team can speak to how different regulatory obligations (federal, state, regional) will intersect with the framework selected.

- **Compliance (i.e., internal audit, risk management)**—Compliance functions such as risk management and internal audit are very familiar with the regulations and frameworks already being followed within an enterprise. They also have extensive experience with testing and validation, documentation, retention, remediation verification, and compliance reporting and presentation—skills that can be leveraged when evaluating and implementing frameworks. (Although the internal audit function can offer important insights during the selection process, it is important that these individuals are not involved in activities that may affect their independence down the road.)

- **Key business process owners**—In addition to the previously mentioned parties, a number of other business functions—typically, those that handle personal information—are impacted by data privacy decisions. These functions vary by enterprise, but marketing and human resources (HR) are often most directly affected. Including them from the start may ensure a smoother adoption.

Including a range of business functions in the selection process is important, but there must be someone included with the authority to make the final decision. This authority will vary, based on organizational structure and maturity, but it should be someone who is very involved in privacy efforts. In some enterprises, this might be the chief privacy officer (CPO); in others, it might be the leader of compliance or risk management. But, as with any committee or team arrangement, there needs to be one person in charge of weighing opinions and making decisions.

---

**Figure 2—Benefits of a Privacy Framework**

The benefits listed include:

- **Effective Evaluation**
- **Risk Mitigation**
- **Measurable Results**
- **Sustainable Program**
- **Privacy, Security, Compliance Unified**
- **Reduced Costs**
- **Streamlined Compliance**
- **Enterprise Strategy**

These benefits are interrelated, forming a cycle that represents the continuous improvement and effectiveness of a privacy framework.
Question 2: How Would a Framework Benefit the Enterprise?
To guide the selection process, the selection team should identify the privacy challenges the enterprise is facing and how a framework could address them. Having a clear understanding of issues and solutions can aid in both selection and implementation. Each enterprise has a different set of problems, and each framework may provide different advantages. A few of the potential benefits include streamlined compliance, measurable results, reduced costs and improved risk mitigation (figure 2).

Question 3: Which Business Operations Will Be Impacted?
When selecting a framework, it is critical to know which business operations (e.g., industry, compliance efforts already in place, geographies) will be within its scope. Data mapping exercises, discovery sessions and data-flow diagrams can aid in identifying these in-scope operations. Understanding how a framework might support, advance or disrupt current operations can impact the decision of whether to select it. Depending on industry, structure and business model, the in-scope processes will vary, but the selection team will likely need to study the impact on IT, security, marketing, HR and all privacy-specific processes.

Question 4: What Frameworks Are Already Being Used?
Before selecting a framework, the selection team must be aware of the frameworks already in place within the enterprise. Frameworks already being utilized could include ISO 29100, FIPPs, or the Generally Accepted Privacy Principles (GAPP). One of these frameworks could serve as a foundation for the adoption process. Further, starting with an already established and adopted framework will help ensure process efficiency. Organizations that would like to mature their privacy programs could consider mapping the privacy frameworks to the cybersecurity frameworks. The team should pay special attention to cybersecurity frameworks (e.g., NIST CSF, NIST SP 800-53, ISO 27001) with the privacy counterparts (e.g., NIST Privacy Framework, ISO 29100).

Question 5: What Regulations Need to Be Considered?
For many enterprises, privacy has traditionally been driven by regulations such as GDPR, CCPA and the US Health Insurance Portability and Accountability Act (HIPAA). Many of the available frameworks intersect with the requirements and principles found in these regulations. By understanding the organization’s regulatory landscape, the selection team can choose a framework that aligns with these requirements, streamlining compliance efforts. However, if regulations are ignored, the framework will become yet another burden on top of current regulatory challenges.

Armed with the answers to these five questions, the selection team should be ready to start evaluating frameworks to find the best fit for the enterprise.

Evaluating and Selecting a Framework
When evaluating frameworks, there are many organizational factors to consider. The most important consideration is: Does this framework support enterprise objectives? Above all else, the selected framework should align with enterprise goals, organizational strategy and stakeholder needs. If it fails to align with any of these elements, enterprise-wide adoption will be difficult, inhibiting the framework’s success.

For example, an enterprise may want to invest in strengthening consumer relationships. The right framework can improve customer trust by simplifying consumer request processes, reducing privacy risk and providing individuals with more control over their information.

Keeping these goals in mind, the selection team can start the evaluation process.

Finding the Right Fit
During the evaluation period, the selection team should determine whether a framework is the right fit for the enterprise, based on its industry, its size and the maturity of its operations. Maturity is an essential consideration. Enterprises should ask: How robust are the processes for data collection, management, storage and transfer? Are privacy and security controls in place to protect these data? Are there...
policies governing these processes? Do the policies and procedures comply with relevant regulations? Beyond operational considerations, enterprises should ask: Are the right skill sets supporting these processes? Is there enough staff to implement and align current operations with this framework? Will this framework empower or inhibit the privacy team?

Enterprises that take a compliance-first approach to privacy can develop a pass-or-fail mentality. However, privacy is an ever-evolving discipline, and it is important to focus on maturing the privacy program, not just checking the right boxes. The selected framework (or frameworks) should serve as a tool to continuously monitor privacy policies and practices and identify opportunities to advance components of the program when appropriate.

Every enterprise is unique, but the good news is that frameworks are designed to be general in nature, so their concepts and principles can be applied to a wide variety of enterprises.

There May Be More Than One Right Answer
With a number of frameworks to choose from, many enterprises struggle to find one that fits to a tee. This is not unusual. However, instead of tailoring the framework to fit the enterprise, many try to squeeze their organizational processes into the framework. This is a mistake.

The best approach is to find a framework that aligns reasonably well with the industry, goals and maturity of the enterprise. Alignment between the objectives of the enterprise and the objectives of the framework is critical. Then the selection team should begin a series of assessments to identify operations or risk factors that do not fall within the framework. Parts of other frameworks can then be adopted to address these areas, or the enterprise can design additional controls that apply to them.

This could also be an opportunity to examine existing enterprise frameworks to determine whether they address any of these areas. This is a key advantage to choosing a privacy framework that integrates well with other frameworks. For example, the NIST Privacy Framework is closely linked to the NIST CSF and NIST SP 800-53. All three use the same structure, making alignment easy. Although the privacy framework may not offer detailed descriptions of data security measures, corresponding sections of the cybersecurity framework do. Choosing a privacy framework with a complementary cybersecurity framework may offer a greater degree of flexibility, extendability and consistency.

It is also critical not to react to every new privacy regulation that surfaces, as this approach may lead to more costs or significant changes to the business environment. The chosen framework (or frameworks) should provide a holistic view of privacy within the enterprise, identifying overlap among various privacy regulations and then aligning them based on the organizational environment (i.e., where data are processed).

Adopting a Framework
As with any integration project, there is no one-size-fits-all approach to adopting a privacy framework. As with every other aspect of the process, how a framework is integrated into the enterprise varies by industry, maturity and organizational culture. However, the integration team can take four steps to ensure that the implementation goes smoothly (figure 3).

Step 1: Map Framework and Regulations
If the enterprise has selected multiple frameworks or if it has a number of regulations with which it must comply, overlap is likely. Mapping out control areas and grouping them by regulation and framework can reduce the complexity. It can also identify gaps in a framework and ensure alignment with compliance requirements. Compliance-focused teams (e.g., internal audit, risk management) can leverage their experience and expertise to guide framework mapping.

Step 2: Tailor to the Enterprise
Tailoring the framework to an enterprise’s specific privacy concerns and regulatory requirements will make adoption smoother. When a framework is adapted to the enterprise, it is easier for stakeholders to integrate it into business operations. Modifying controls with specific functions to align with the enterprise and with the information systems and the operating environment will make the framework easier to apply.

Step 3: Document
There may be instances when a specific control area in a framework does not apply to an enterprise. In these cases, it is best to document the business and technical reasons why the enterprise chose not to use that specific control area. The team should not just ignore that section of the framework. Having appropriate documentation of the reasoning
behind each exception will assist during audits and assessments. In addition, documentation is vital to providing transparency and understanding of the enterprise’s operations and strategies.

**Step 4: Communicate and Project Management**
As with any project, communication is critical to a successful framework adoption. Information about new frameworks should be communicated early so that core functions know to expect changes. Frequent communication is vital; sending regular updates and reminders keeps the framework adoption foremost in people’s minds. Transparency is also key. If changes have to be made as a result of adopting the framework, the implementation team should not hide this from stakeholders. By being up-front about changes, the team can get the appropriate support to ensure that adoption goes smoothly.

**Conclusion**
Having a privacy framework in place speaks volumes to an enterprise’s investment in and prioritization of data protection efforts. However, it is not enough to simply have the framework’s recommendations and related controls written down on paper. The enterprise must have robust processes in place to implement, manage and enhance these controls and ensure their effectiveness. Whichever framework or combination of frameworks an enterprise chooses, it must have a comprehensive strategy in place to carry out the framework’s recommendations for protecting personal information and ensuring data security.

**Endnotes**