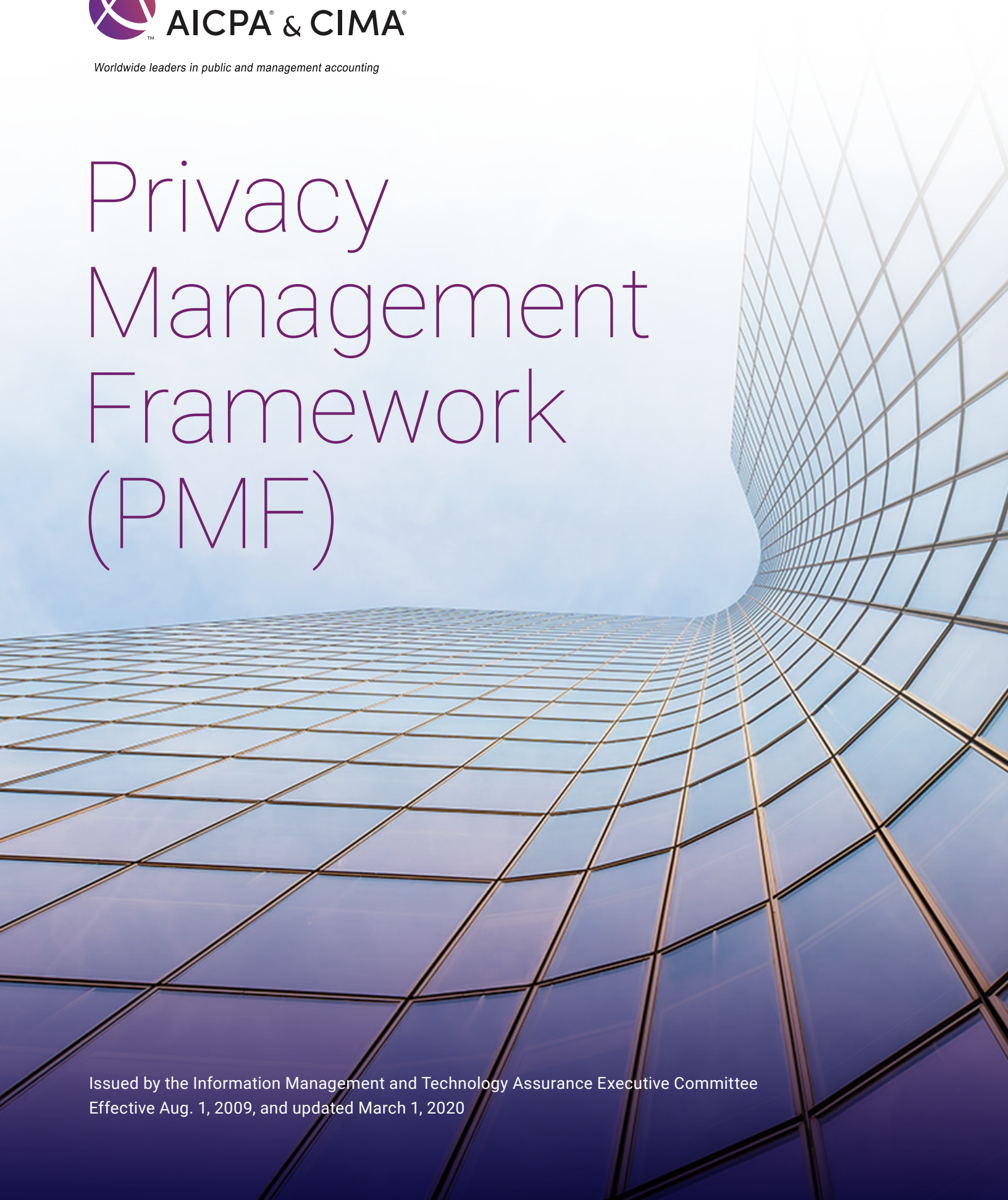
Technology

AICPA & CIMA

Worldwide leaders in public and management accounting

Privacy Management Framework (PMF)



Issued by the Information Management and Technology Assurance Executive Committee
Effective Aug. 1, 2009, and updated March 1, 2020

Contents of framework

History and ongoing process

First created by the American Institute of CPAs® (AICPA®) and the Canadian Institute of Accountants (CICA), the original framework was published in November 2003 and revised in March 2004 under the name AICPA/CICA Privacy Framework. Later, in August 2009, the framework was revised and renamed Generally Accepted Privacy Principles (GAPP). And, in 2020, the GAPP was updated again and renamed the Privacy Management Framework (PMF).

Because of significant changes in technologies and in global, country-specific and local information and data privacy laws and standards, including the publication of the General Data Protection Regulation (GDPR) and updates to the AICPA's Trust Services Criteria (TSC), the AICPA Privacy Task Force updated this PMF document in 2020. Members of this task force brought subject matter expertise in data privacy and recognized changes to international and U.S. privacy requirements and best practices, as well as the evolving privacy expectations of consumers and individual data subjects.

For entities operating in multijurisdictional environments, managing privacy risk presents unique challenges. For that reason, applying the concepts and practices included within this updated PMF cannot guarantee an entity's compliance with the various privacy laws and regulations for which an organization is subject. Organizations need to be aware of the privacy requirements in the jurisdictions in which they do business. Since the updated PMF provides guidance on privacy, in general, organizations should always seek sound legal counsel regarding the specific laws and regulations impacting the organization's unique facts and circumstances.

This updated PMF has been approved by both the AICPA Privacy Task Force and the AICPA Information Management and Technology Assurance Executive Committee. The adoption of the PMF is voluntary.

Because the topic of personal information (PI) and data privacy is constantly changing, the PMF will need to be periodically revised. Accordingly, please email any comments about this framework to IMTAinfo@aicpa.org.

Introduction

Nature of the analysis

The Privacy Management Framework (PMF) is designed to assist management in creating an effective information privacy program that addresses privacy obligations and risks, while facilitating current and future business opportunities. By using the PMF, organizations/entities (both terms used interchangeably) can proactively address the significant challenges that they face in establishing and managing their privacy programs and risks from a business perspective. The PMF also facilitates the management of privacy risk on a multijurisdictional basis.

There continue to be increased public demands that organizations strengthen the effectiveness of their data security controls — those operating within and those surrounding the systems used to collect, process, create and store personal information (PI) and the sensitive information of customers, employees and others with whom they interact. This is a direct reaction to numerous publicized instances where significant amounts of PI have been extracted from systems and either sold on the internet or used to steal an individual's identity. As a result, many countries have begun to enact laws that affirm the rights of citizens as the owners of their unique PI, and provide citizens with remedies when organizations collect, create or use a person's PI without their permission, or for purposes for which an individual has not given permission.

These laws have confirmed individual citizen's expectations of privacy when it comes to business transactions and agreements and require organizations to inform individuals that they have options when it comes to sharing their PI. The advent of electronic commerce also ushered in an era where businesses engaged in commerce over the public internet often need to collect PI from customers to validate their identities and their agreement to buy or consume a service in an arm's-length transaction. As individuals have become more concerned about their privacy, and the details about themselves others might be able to learn, many have sought to not convey information about themselves to organizations and, in some situations, to their governments without some guarantee that the PI will only be collected, created, used, stored and transmitted with their explicit permission, and for the purposes necessary for its collection and use.

With people more interested in protecting their anonymity, such people or data subjects (e.g., the legal and human person whose personal details are the subject of privacy concerns as opposed to legal non-human persons such as trusts, corporations, etc.) expect that data and information about their physical person, health, financial condition, religious and political beliefs, opinions, likes and dislikes and, ultimately, their personal data, remain in a protected private state under their ultimate control. In the PMF, we will use the term PI to describe both personal data and information.

Why information and data privacy are an enterprise concern

It is commonly understood that effectively executing enterprise information and data security and privacy practices is a required and expected practice for any organization that depends on network and internet-connected computing and data storage technologies. Executing effective data privacy protection practices is also a key part of an organization's governance and accountability setting activities.

As systems and technology-enabled business processes continue to evolve and become increasingly complex and sophisticated, many organizations struggle to get their hands around the growing amounts of PI they collect and need to operate effectively. That's because PI is valuable, but its value is not recorded in financial terms. And, like other corporate tangible assets like cash, securities and inventory, PI and business-sensitive information is also highly vulnerable to the risks from theft, misuse, unauthorized access, alteration and in the case of PI, illegal disclosure. Added to that risk, PI exposes organizations to the risk of financial penalties and sanctions, the effects of bad publicity, and the potential for increased regulatory scrutiny and government sanctions if such risk events happen. Thus, an organization's IT security programs, and the way it evaluates risks, known problems and vulnerabilities, increases the concerns organizations, governments and the public have related to data privacy. And, as a result, organizations need to elevate and effectively address information privacy as an enterprise risk that must be recognized, understood, evaluated and managed.

Organizations also need to strike a balance between their need to collect, manage and use PI when providing services and the nature, costs and types of privacy controls that would be most appropriate to design and execute these activities.

When individuals engage organizations for the provision of products and services, they generally agree to provide their unique PI as part of the exchange. This might be when they seek to obtain or accept a vendor's product warranty coverage or limitations, or warranty services after the product purchase. In this example, customers generally will agree to provide their PI to the product's manufacturer or reseller organization, but they also expect that their rights to privacy will be protected, and their PI will only be used for the purpose for which it was provided. In this example, the product manufacturer or reseller needs to authenticate the identity of the product's purchaser and their warranty coverage. In this example, a purchaser may also have an expectation of privacy in their PI, and that expectation flows to the holders of the PI and any other organization that may have been given access to the information, such might be the case with a third-party vendor of the manufacturer or reseller organization entrusted to process and manage the PI.

The customer expects that their PI will be kept securely, protected from unauthorized access and used and monitored for indications of theft and possible misuse. Because of the increased demands of new data privacy legislation and changes in public opinion about the topic, individuals and regulators are no longer willing to overlook an organization's failure to protect the privacy of the PI that was entrusted to their care.

The following are some privacy risks that are caused by ineffectively designing and operating privacy policies and procedures:

- Damage to the organization's reputation, brand or business relationships
- Legal liabilities and industry or regulatory sanctions
- Charges of deceptive business practices
- Customer and employee distrust
- The denial of data subject consent to share PI required for a stated business purpose
- Loss of business and its consequential reduction in revenue and market share
- Disruptions to international business operations
- Legal costs of recovering from identity theft and making injured parties whole

Application and impacts on governments and privacy laws

This PMF applies to (legal) commercial business entities with which individuals execute agreed business transactions, as well as medical and legal professionals who have a fiduciary duty to serve the needs of clients and to keep details of their engagements privileged, confidential, protected and private.

The PMF also applies to government agencies that serve the broader needs of society. That is why laws, including the U.S. Health Insurance Portability and Accountability Act (HIPAA) and recently enacted regional laws such as the European Union's (EU) General Data Protection Regulation (GDPR) and the state of California's Consumer Privacy Act (CCPA), affirm the rights of each citizen or data subject. These laws describe the duties and responsibilities of both the data subject and commercial entities to which they have given their explicit permission to collect, use, create, store, access, manage, process and control PI to facilitate transactions for commercial products and services. In these situations, data subjects might seek a product or service and, to execute a transaction and exchange of value, the business entity agrees to sell the product or service to a data subject in exchange for valuable consideration, including payment and data or information to continue to provide support for either or both the product or the service.

Moreover, under newly stated and fundamental rights of identity self-ownership, these new laws not only codify the rights of data subjects to the control of their identities, but they also outline the legal obligations organizations must acknowledge and follow when they seek to collect, create, process, hold, use or share a data subject's PI. These new regulations will shape the way businesses and other organizations deal with PI, but they also recognize that before an organization collects, creates, processes, holds, uses or shares an individual's PI, there must be an upfront explicit (in writing or electronically signed) agreement between two parties for the exchange of something of value. In this case, the value exchange is a data subject's PI for some good or service (of value to each). These laws mandate that organizations that collect and use PI, only use PI for the purposes for which they initially agreed with data subjects to collect and use their PI. Further, these regulations now require that other data controllers and processors of PI notify data subjects (and, in some cases, specific legal authorities) when those organizations determine that PI entrusted to their care has been stolen or taken from the organization without the permission of the data subjects in question.

Recent data breaches show that most data subjects also have an expectation that they will be notified and made whole for the loss of their PI and for any subsequent and actual losses or damages they might have, whether these are calculated in purely financial terms. For these reasons, information and data privacy and computer security continue to be top of mind for individuals, organizations and governmental bodies.

The 2018 enactment of the GDPR not only forces organizations to follow strict data handling and privacy requirements, but it also puts individual data subjects in control of their PI, and it does so in a way that will influence similar legislation in other jurisdictions. The GDPR specifies what an organization must do if it wants to collect, create, process, hold (store), use or share an EU citizen's data. It also prescribes requirements as to how and under what circumstances and what purposes an EU citizen's data can be collected, processed and used, and it allows data subjects the right to get a complete accounting of all the personal data an organization possesses about themselves, and to request the organization remove and erase the data if the subject wishes.

The regulation also defines privacy concepts and principles, establishes roles of organizations that control and process the data and sets rules about who and which organizations the data can be shared with and for what purposes, and it allows data subjects to be "forgotten." Finally, the regulation sets high expectations regarding the fiduciary duties of data processors, controllers and other third-party service organizations that might encounter PI either directly or indirectly.

Because of these new requirements, organizations are being forced to take an in-depth look at the way they interact with EU citizens and residents of the State of California. This is especially important when organizations use technology to capture and record a prospective customer's PI, or track a prospective customer's browsing and searching habits, or when their systems were originally designed to monitor user behaviors and offer goods and services to a user of the organization's systems (which is disallowed for users who are EU citizens without their explicit consent).

International data privacy considerations

For organizations operating in more than one country, the management of privacy risks can be significantly challenging. The global internet and connected business systems mean that regulatory requirements or actions of one country can affect the rights, duties and obligations of individual users and organizations operating around the world. Many individual and united countries have laws regulating trans-border data flows of citizen PI of which an organization must comply if the organization wants to do business in these countries. Some jurisdictions apply different legal concepts and precepts when it comes to privacy, making compliance in and across borders more complex.

To illustrate, some nation's laws say PI belongs to the individual citizen from whom it relates and take the position that the entity that collects it has a legal and fiduciary duty when managing and using it. Some countries view PI as belonging to the enterprise that collects it. Finally, legal jurisdictions (e.g., countries, states or provinces) and even certain industries such as healthcare and banking, have their specific requirements related to information privacy.

Outsourcing and information privacy

Outsourcing the management and operational support for systems and data processing to others, such as in a service platform, infrastructure and data management, and for applications that rely on cloud computing technologies, increases the complexity of an organization's ability to address its information privacy requirements. Organizations are also increasingly looking to move computing and data storage to other organizations or to outsource business processes and, with it, the activities related to information privacy. However, outsourcing organizations cannot delegate their responsibilities for protecting the privacy of data subjects and their identifying information related to its business processes and practices. Complexity also increases when the entity that performs the outsourced service is located or operates in a different country and may be subject to different privacy laws or perhaps no privacy requirements at all. In such circumstances, the organization that outsources a business process will need to make sure it manages its privacy responsibilities appropriately.

The PMF and its supporting criteria can assist an organization in completing assessments about the privacy policies, procedures and practices of the third party providing the outsourced services.

The fact that the PMF has a global application can provide comfort (e.g., assurances) to an outsourcer that privacy assessments can be undertaken using a consistent measurement based on internationally known fair information practices.

Important updates to the framework

Because of recent changes and recognizing that the 2009 framework did not reflect global realities or the evolving needs of users, it was an appropriate time for the framework to be updated. The updated PMF aligns and links common information privacy requirements into a set of unique objectives supported by nine core components. Each privacy component is supported by a relevant objective and measurable criteria and form the basis for an organization's effective management of the risks to information privacy and their continued adherence to regulatory change. In addition to the criteria, the PMF presents points of focus for each criterion. Some of the points of focus may not be directly applicable to each organization or its internal business-related processes. When a criterion is determined to be inapplicable, the entity should document its rationale in a way that supports future privacy evaluations. These points of focus provide a basis for designing, implementing, maintaining, evaluating and auditing a privacy program to meet an entity's unique needs and requirements. Wherever possible, the PMF was aligned with Trust Services Criteria (TSC) and, therefore, the terminology is very similar between the former Generally Accepted Privacy Principles (GAPP), TSC and the new PMF.

An important update to the PMF is the replacement of the "choice and consent" component. While the choice and consent criteria were relevant to internet-oriented businesses in 2009, the criteria are much less relevant today because of new global privacy regulations such as the GDPR. In this update, the framework recognizes that underlying any exchange of PI are business transactions, and the recognition that such transactions are implicit and, in many cases, explicit agreements that are generally bound by laws and regulations. As such, this new guideline recognizes that the parties to a transaction have agreed to an exchange of value and, in doing so, have given their consent. Therefore, choice and consent were present so the transaction could be fully executed. This update to the PMF focuses on situations when an individual has provided their PI to an organization and, where in the past, choice and consent might have been viewed as separate aspects of the core privacy criteria instead of as the underlying transactions that caused the individual to be a principal interest to those entities.

As with the original 2009 framework, this updated version can be used as a foundational element in establishing and operating a comprehensive information privacy program. Applying the PMF to a business or a non-profit entity's systems and processes can help management identify and address legal and data privacy risks, continue to satisfy the changing expectations of data subjects, customers, users and regulators, and help the organization achieve its stated privacy obligations and commitments. Applying the framework also helps establish leadership and customer trust in an entity's practices that generate future business opportunity. The PMF should be a useful tool for boards and others who are charged with governance and the independent oversight and monitoring of an entity's operations.

The PMF explains why privacy is an enterprise risk management issue rather than just an IT, legal or compliance issue. The PMF will help those involved in:

- overseeing and monitoring information privacy and IT security;
- implementing and managing legal, regulatory and compliance activities related to privacy;
- operating customer-facing (i.e., online or in-person) business processes;
- evaluating and managing enterprise risk management programs and activities;
- auditing IT systems, information privacy, data protection and security controls; and,
- implementing public policy that addresses information and data privacy concerns.

Overall privacy objective

The PMF components are founded on the following privacy objective:

> Personal information (PI) is collected, created, used, processed, retained, disclosed and disposed of in conformity with agreements made between data subjects and users of the entity's products and services, and found in the entity's formal privacy notices and communications and with criteria outlined in the PMF issued by the AICPA.

Components of the framework

The nine components of the PMF are as follows:

1. **Management** — The entity defines, formally documents, communicates and assigns responsibility and accountability for its PI privacy policies and procedures.
2. **Agreement, notice and communication** — The entity makes formal agreements, notifies and communicates with and offers choices when seeking data subject consents, including reasons why and purposes for which the entity seeks to obtain and use a data subject's PI.
3. **Collection and creation** — The entity collects and creates PI only for the purposes identified in its agreements with data subjects, and in ongoing communications with and notices provided to data subjects.
4. **Use, retention and disposal** — The entity limits the use of PI to the purposes identified in the formal agreements/notices, and for which a data subject has provided explicit (or implicit) consent. The entity retains PI for the time necessary to fulfill the stated purposes identified in the formal agreements/notices or as required by laws or regulations. Once those purposes have been met, the entity securely disposes of the information.
5. **Access** — The entity provides data subjects with access to their PI when requested or when asked to update and correct data errors or make changes.
6. **Disclosure to third parties** — The entity discloses PI to third parties only for the purposes identified in data subject privacy agreements and its privacy notice and with the explicit consent of the data subject.
7. **Security for privacy** — The entity protects PI against unauthorized access, removal, alteration, destruction and disclosure (both physical and logical).
8. **Data integrity and quality** — The entity maintains accurate, complete and relevant PI for the purposes identified in the notice and protects the representational integrity of the PI in its ongoing interactions with data subjects.
9. **Monitoring and enforcement** — The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

Illustrations and uses

The following summarizes and illustrates how the PMF can be used by organizations to address the business activities that involve collecting, creating, using, storing and transmitting the PI of individuals.

Some of the points of focus may not be directly applicable to each organization or its internal business-related processes. When a criterion is determined to be inapplicable, the entity should document its rationale in a way that supports future privacy evaluations.

These points of focus provide a basis for designing, implementing, maintaining, evaluating and auditing a privacy program to meet an entity's unique needs and requirements.

Strategy development	
General discussion	Potential use of the PMF
• **Vision** — An entity's business strategy is concerned with the organization's primary objectives, direction and prosperity. An entity's privacy strategy is concerned with its objectives, goals and desired outcomes related to protecting the privacy of PI. A vision statement expresses aspects of the organization's operating style and culture and helps shape and determine how it will interact within the markets in which it operates, including with its customers, competitors and in consideration of legal, social and ethical issues. • **Strategic plan** — This is an entity's overall plan for achieving the vision it has set for itself by executing the business activities underlying its strategic direction. The objectives in doing so are designed to help make sure that an entity's efforts are directed towards a common purpose and direction. • **Resource allocation** — This activity helps the organization appropriately use, manage and allocate available human, financial and intellectual property assets and resources in support of the achievement of its goals and objectives, and as outlined in its strategic and tactical business plans.	• **Vision** — An entity's privacy efforts can be aligned with an entity's strategy and vision and can help the entity establish and follow practices that connect the protection of PI of employees and customers (and other stakeholders) with its business strategy, markets and business model. • **Strategic plan** — Within an entity's privacy effort, the PMF can be used to help guide the organization in establishing necessary policies, procedures, practices and communications that will signify the entity's commitment to protect the integrity, confidentiality and reliability of essential PI it needs to operate its business activities. • **Resource allocation** — Using the PMF, the entity would identify the people working with and responsible for areas that might include systems management, privacy and security concerns, and stipulate the resourcing for their activities. • **Overall strategy** — A strategic document describes expected or intended future development. The PMF can assist an entity in clarifying plans for the systems under consideration or the business' privacy objectives. The plan identifies the process to achieve goals and milestones. It also provides a mechanism to communicate critical implementation elements, including details on services, budgets, development costs, promotion and privacy advertising.

Internal privacy risk assessment

General discussion	Potential use of the PMF
• **Assessment** — This stage covers the thorough analysis of an entity's computing and data collecting, creating, using and protection activities and technologies, and the way unauthorized access to user PI is prevented or detected, or where opportunities exist for insiders or outsiders to exploit weaknesses in systems or defeat controls. This includes where known problems, vulnerabilities and present threats are observable but are not being addressed or mitigated effectively. • **Diagnostic evaluation** — The most common initial project for an organization is an in-depth diagnostic evaluation. The purpose of the evaluation is to identify and observe how the entity has assessed the risks it faces due to the way it operates, the value of its information assets, how it set its information privacy objectives relative to its regulatory and financial risk thresholds, and the extent to which the organization can achieve those objectives given how it operates and secures its systems and data.	• **Strategy** — The PMF can assist the entity in understanding its high-level risks, opportunities, needs, privacy policy and practices, competitive pressures and the requirements of the relevant laws and regulations to which the entity is subject. The PMF provides a legislative neutral benchmark to allow the entity to assess the current state of privacy against the desired state.

Implementation

General discussion	Potential use of the PMF
• **Action plan** — At this point, an action plan is mobilized, or a diagnostic recommendation is put into effect or both. Implementation involves developing and documenting a privacy program and action plan and the execution of all planned and other tasks necessary to make the action plan operational. It includes defining who will perform what tasks, assigning responsibilities and establishing schedules and milestones. This involves the planning and implementation of a series of projects to provide a framework, direction, methodology and tools to the organization in developing its initiatives.	• **Completion** — The PMF can assist the entity in meeting its implementation goals. After the implementation phase, the entity should have developed systems, procedures and processes to address its privacy requirements. The entity should have updated privacy-compliant forms, brochures and contracts and should have internal and external privacy awareness programs.

Monitoring

General discussion	Potential use of the PMF
• **Sustain** — Sustaining and managing involve monitoring the work to identify how progress differs from the action plan to initiate corrective action. Monitoring refers to the management policies, processes and supporting technology to make sure compliance with organizational privacy policies and procedures and the ability to exhibit due diligence.	• **Sustain** — The entity can use the PMF to develop appropriate reporting criteria for monitoring requests for information, the sources used to compile the information and the information disclosed. It can also be used for determining validation procedures to make sure that the parties to whom the information was disclosed are entitled to receive that information.

Internal audit

General discussion	Potential use of the PMF
• **Manage internally** — Internal auditors provide an entity's board of directors with assurances regarding the protection of an entity's resources including the protection of PI that is critical to the entity's performance. This includes the appropriateness of the use of the entity's resources according to the entity's organizational governance requirements and mandates, and to applicable regulations and law. Internal audit functions can help an entity accomplish its stated business objectives by applying recognized, systematic, disciplined approaches to the evaluation and improvement of an entity's operations, assessments of the effectiveness of risk management, internal control, and resource management processes.	• **Manage internally** — Internal auditors can actively participate in an organization's ongoing evaluations of information security, data privacy and related internal control activities and technologies. Auditors can use the PMF as a benchmarking tool that offers users important information about reporting on the sufficiency of an organization's information privacy activities to boards and executive managers.

External audit

General discussion	Potential use of the PMF
• **Manage externally** — External auditors, notably Certified Public Accountants (CPAs), can perform attestation and assurance services. Generally, these services, whether performed on financial or nonfinancial information, build trust and confidence for individuals, management, customers, business partners and other users.	• **Manage externally** — External auditors can use the PMF in independent and separate evaluations of an entity's privacy program, practices and controls and help auditors report on activities related to individuals, management, customers, business partners and other users.

Privacy Management Framework mapping tool

The following Privacy Management Framework (PMF) mapping tool provides general guidance on privacy and is intended to help practitioners and users effectively manage their privacy risks and comply with applicable privacy laws.

This tool maps each of the nine components of the PMF with Trust Services Criteria (TSC) and the European Union (EU)'s General Data Protection Regulation (GDPR). Practitioners should customize this tool to meet their needs. For example, consider adding sections to address specific organizational policies and document how such policies compare to the PMF and industry standards and laws.

Organizations should always seek sound legal counsel regarding the specific laws and regulations impacting their unique facts and circumstances.

A downloadable Excel version of this resource is available on AICPA.org/IMTA to allow users to customize the resource for their specific needs.

Management

PMF ref. #	Components of the PMF	TSC relevant references	GDPR article references
M1.0	Management	N/A (general)	Articles 5, 6, 24, 27, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40

M1.0 The entity has defined and formally documented data and information privacy policies and procedures for PI collection, usage and processing that are consistent with the entity's objectives related to privacy.

Agreement, notice and communication: The entity has formal agreements, provides notices and formally communicates with data subjects about its privacy practices to meet the entity's objectives related to privacy. Refer to Component N2.0.

Collection and creation: The entity has defined policies and procedures for collecting and creating a data subject's PI. Refer to Component C3.0.

Use, retention and disposal: The entity has policies and procedures for handling PI to achieve the stated purposes and needs for which the PI was initially collected. Refer to Component U4.0.

Access: The entity has policies and procedures for viewing, inspecting, accessing and modifying PI. Refer to Component A5.0.

Disclosure to third parties: The entity has policies and procedures for disclosing and transmitting PI to external third-party individuals and organizations not under the direct management or control of the entity. Refer to Component D6.0.

Security for privacy: The entity has policies and procedures for protecting the integrity of PI during initial and subsequent collection, creation, usage, processing, alteration, adaptation, re-organization, storage, destruction and erasure. Refer to Component S7.0.

Data quality and integrity: The entity has a process for preserving and periodically re-validating the quality and integrity of PI and verifying (e.g., confirming with data subjects) its continued accuracy, completeness and correctness. Refer to Component Q8.0.

Monitoring and enforcement: The entity has processes for assuring adherence to information privacy policies and procedures through ongoing and separate evaluations. Refer to Component M9.0.

PMF ref. #	Components of the PMF	GDPR article references
M1.2	The entity has implemented a policy governance and accountability process that defines and formally documents policies and procedures for information privacy that are consistent with the entity's objectives related to privacy.	
Points of focus	**Responsibility and authority:** The entity has an overall governance and legal structure that defines and establishes responsibility and authority for the entity's oversight processes, policy setting and ongoing monitoring activities.	Articles, 27 (1); 37 (1), (2), (3), (4), (6); 38 (1), (3); 39 (1), (2)
	Established accountability: The entity has a governance and legal structure that establishes accountability for information privacy policy creation, oversight, monitoring and compliance.	Article 24 (2)
	Privacy awareness and training: The entity provides a privacy awareness program about its privacy policies and related matters, and provides specific training for selected personnel depending on their roles and responsibilities.	
	Qualifications of internal personnel: The entity establishes qualifications for personnel responsible for protecting the privacy and security of PI and assigns such responsibilities only to those personnel who meet these qualifications and who have received training.	Articles 37 (5); 38 (2)
	Policy changes: The entity has a process for evaluating and addressing the potential impacts of required changes to information privacy policy and procedures as changes occur in entity operations and operating locations, and as applicable jurisdictional laws and regulations are enacted to become new regulatory compliance requirements.	Article 6 (4)
	Oversight and monitoring: The entity has a process for governing and overseeing the application of policies and procedures.	Articles 27 (1), (2), (3), (4), (5); 31; 38 (3), (5)
	Policy compliance: The entity has procedures for identifying and addressing instances when non-compliance with information privacy policies and procedures are identified.	
	Policy communications: The entity communicates its information privacy policies to internal personnel and other external third parties engaged in providing business process, IT services and information privacy support.	
	Consistency of commitments with privacy policies and procedures: The entity's internal personnel or advisers review contracts for consistency with privacy policies and procedures and address any inconsistencies.	

PMF ref. #	Components of the PMF	GDPR article references
M1.3	The entity has established policies and procedures for identifying, classifying and prioritizing the criticality of its collected PI. The entity also has procedures for evaluating potential vulnerabilities and the risk of unauthorized privacy information access, removal and destruction. The entity has designed and implemented control activities to help prevent, detect, address and notify relevant authorities in the event it detects and confirms instances of system and privacy information breaches. These policies and procedures were designed to help the entity meet its objectives related to privacy.	
Points of focus	Data and information classification: The entity has a process for classifying PI according to applicable regulation and risks associated with unauthorized disclosure or misuse.	Article 30 (1), (2), (3), (4), (5)
	Privacy (risk) impact assessment: The entity performs a privacy (risk) impact assessment to identify and evaluate privacy specific risks, vulnerabilities and scenarios that could result in a system or information privacy breach situation. Privacy (risk) impact assessments are also used to identify security control weaknesses that need to be addressed as well as to report upon the entity's ability to comply with applicable system and privacy information breach notification laws and regulations.	Articles 35 (1), (2), (3), (4), (5), (7), (8), (10), (11); 36 (1), (2)
	Privacy incident response plan: The entity has a comprehensive privacy incident and breach management plan which provides examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The plan is communicated to personnel who handle PI.	Articles 5 (1) (f); 33 (1), (2), (3), (4), (5); 34 (1), (2), (3), (4)
	Ongoing and separate evaluations: The entity has a process for performing ongoing and separate evaluations of the design and operating effectiveness of information privacy and security controls and for addressing any identified control deficiencies.	Articles 32 (3); 40 (1), (2), (3), (4)
M1.4	The entity has a process for identifying, locating and classifying its PI. This process is clearly described as an essential aspect of its data governance program which is aligned with its information security controls. Relevant control activity policies and procedures have been designed and placed into operation to achieve the entity's objectives related to privacy.	
Point of focus	Data privacy security controls: The entity has a process to identify the specific or key data privacy security controls that it has designed and placed into operation that help reduce the risks of a data breach or a theft, erasure or alteration of PI.	Article 32 (1), (2)

Agreement, notice and communication

PMF ref. #	Components of the PMF	TSC relevant references	GDPR article references
N2.0	**Agreement, notice and communication**	P1.0, *Privacy criteria related to notice and communication of objectives related to privacy* P2.0, *Privacy criteria related to choice and consent*	Articles 12, 13, 14, 15, 18, 21
N2.1	The entity executes formal agreements, provides notices and formally communicates with data subjects about its privacy practices to meet its objectives related to privacy.		
Points of focus	**Agreements, notices and communications:** The entity's agreements with data subjects formally capture data subject consents for sharing their PI with the entity and third parties affiliated with the entity, and for situations where the entity assembles, creates or purchases a data subject's PI, and when the entity needs to change the original purposes for obtaining a data subject's PI to meet the entity's changing business, operational or legal requirements.		Articles 12 (1); 14 (1), (2), (3), (4), (5); 15 (1), (2); 18 (3)
	Ongoing notices and communications: The entity has a process for periodically informing data subjects of its continued need for PI. The entity also has a process for obtaining the data subject's continued agreement and consent to use the data, and for informing data subjects when the entity suspects or learns, through ongoing monitoring and testing, that its systems (and systems of third parties providing services to the entity) have been breached and PI has been accessed, altered or removed in an unauthorized manner.		Articles 13 (2), (3); 21 (4)
	Entities and activities covered: The entity has an objective description of the entities and activities covered by the privacy policies and procedures that is included in the entity's privacy notice.		
	Clear and conspicuous: The entity's privacy notice is conspicuous and uses clear language.		
	Data subject revocations: When required, the entity has a process that provides data subjects a mechanism with which to request the entity to remove, dispose and erase a data subject's PI. Once a data subject's PI is no longer being stored in the entity's systems (this includes other affiliates and third parties that may also hold or store privacy information on behalf of the entity), the entity notifies the affected data subjects that such information has been removed.		

PMF ref. #	Components of the PMF	GDPR article references
N2.2	Changes to privacy agreements are communicated in formal notices to affected data subjects. The updated agreements are re-executed by data subjects to reflect the changes made to the entity's privacy practices. Data subjects are also notified, and the agreements are updated in situations where the originally intended purposes for collecting a data subject's PI need to be updated or changed. Such notifications and communications are consistent with the entity's objectives related to privacy.	
Point of focus	**Changes to privacy agreements/notices:** The entity has policies and procedures it follows when it is determined that changes are needed to its privacy agreements/ notices. The entity documents the reasons for such changes and these changes are formally approved by an authorized member of management prior to being implemented. When required, the entity also notifies affected data subjects and obtains their formal approval (consent) prior to continuing to use or process a data subject's PI.	

Collection and creation

PMF ref. #	Components of the PMF	TSC relevant references	GDPR article references
C3.0	**Collection and creation**	P2.0, *Privacy criteria related to choice and consent* P3.0, *Privacy criteria related to collection*	Articles 5, 6, 7, 8, 9, 10, 11, 21, 25, 49
C3.1	The entity communicates available options regarding the collection and creation of PI and the consequences of each choice, including the data subject's option to reject their agreed consent for the entity to initially or subsequently collect and create PI.		
Points of focus	**Communicates to data subjects:** Data subjects are informed about the choices available to them with respect to the collection, use and disclosure of PI. Data subjects are informed that implicit or explicit consent is required to collect, use and disclose PI, unless a law or regulation specifically requires or allows otherwise.		Article 8 (1), (2)
	Ability to opt-out: The entity has a process to allow data subjects with the option of not providing their PI, according to the data privacy agreement, including notifying the data subjects of the consequences of not agreeing to its provision and use by the entity.		
	Communicates consequences of denying or withdrawing consent: When PI is collected, data subjects are informed of the consequences of refusing to provide PI for purposes identified in the notice.		Article 21 (5)
	PI collection and creation: The entity has a process to collect and create (rendering and aggregating from multiple sources or information providers) PI as identified in the entity's privacy agreements. The process is consistent with its objectives related to privacy.		Articles 5 (1)(b), (1)(c); 9 (2), (3); 10; 11 (1); 25 (2)

PMF ref. #	Components of the PMF	GDPR article references
C3.2	The data subject's agreed consent is explicitly obtained and is only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent, when implicit consent is allowed as an available option, is documented.	
Points of focus	**Documents and obtained consent for new purposes and uses:** If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the data subject is notified, and implicit or explicit consent is obtained prior to such new use or purpose.	Article 6 (4)
	Explicit and implicit consent: The entity's policies and procedures require data subjects to explicitly agree and consent to the provision and collection of the data subject's PI. In some circumstances where the entity is unable to confirm explicit consent directly with a data subject, the entity's policies and procedures require the entity to formally document its rationale and basis for determining that it has obtained the data subject's implicit consent.	Article 7 (1), (2), (3), (4)
	Obtains explicit consent for sensitive information: Explicit consent is obtained directly from the data subject when sensitive PI is collected, used or disclosed, unless a law or regulation specifically requires otherwise.	Articles 7 (3); 49 (1), (2), (3)
	Obtains consent for data transfers: Consent is obtained before PI is transferred to or from an individual's computer or other similar device.	

Use, retention and disposal

PMF ref. #	Components of the PMF	TSC relevant references	GDPR article references
U4.0	**Use, retention and disposal**	P4.0, *Privacy criteria related to use, retention and disposal*	Articles 5, 6, 7, 9, 10, 11, 15, 17, 18, 20, 21, 22, 25, 29, 32, 44, 45, 46, 49
U4.1	The entity limits the use of PI to the purposes identified in its objectives related to privacy.		
Point of focus	**Only uses PI for intended purposes:** PI is used only for the intended purposes for which it was collected and only when implicit or explicit consent has been obtained unless a law or regulation specifically requires otherwise.		Articles 5 (1)(a), (1)(b); 6 (1), (4); 7 (3); 9 (1), (2), (3); 10; 15 (4); 18 (1), (2); 20 (4); 21 (1), (2), (3), (6); 22 (1), (2), (3), (4); 25 (2); 29; 32 (4); 44; 45 (1); 46 (1), (2); 49 (1), (2), (3)

PMF ref. #	Components of the PMF	GDPR article references
U4.2	The entity retains PI consistent with its objectives related to privacy.	
Points of focus	**Retains PI:** PI is retained for no longer than necessary to fulfill the stated purposes, unless a law or regulation specifically requires otherwise.	Articles 5 (1)(e); 11 (1); 17 (1)
	Protects PI: Policies and procedures have been implemented to protect PI from erasure or destruction during the specified retention period of the information.	Articles 5 (1)(f); 25 (2); 46 (1), (2); 49 (1), (2), (3)
U4.3	The entity securely disposes of PI consistent with its objectives related to privacy.	
Points of focus	**Captures, identifies and flags requests for deletion:** Requests for deletion of PI are captured and information related to the requests is identified and flagged for destruction to meet the entity's objectives related to privacy.	Article 17 (1), (2), (3)
	Disposes of, destroys and redacts PI: PI no longer retained is anonymized, disposed of or destroyed in a manner that prevents loss, theft, misuse or unauthorized access.	
	Destroys PI: Policies and procedures are implemented to erase or otherwise destroy PI that has been identified for destruction.	Article 25 (2)

Access

PMF ref. #	Components of the PMF	TSC relevant references	GDPR article references
A5.0	Access	P5.0, *Privacy criteria related to access*	Articles 11, 12, 15, 16, 20
A5.1	The entity grants identified and authenticated data subjects the ability to access their stored PI for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.		
Points of focus	**Authenticates data subjects' identities:** The identity of data subjects who request access to their PI is authenticated before they are given access to that information.		Articles 11 (2), 12 (6)
	Permits data subjects access to their PI: Data subjects can determine whether the entity maintains PI about them and, upon request, may confirm and obtain access to their PI or request that the PI be returned, removed or erased.		Articles 15 (1), (3); 20 (1), (2), (3), (4)
	Provides understandable PI within reasonable time: PI is provided to data subjects in an understandable form, in a reasonable time frame and at a reasonable cost, if any.		Article 12 (1), (3), (8)
	Informs data subjects when access is denied: When data subjects are denied access to their PI, the entity informs them of the denial and the reasons for the denial in a timely manner, unless prohibited by law or regulation.		Article 12 (2), (4), (5)
A5.2	The entity corrects, amends or appends PI based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.		
Points of focus	**Communicates denial of access requests:** Data subjects are informed, in writing, of the reason a request for access to their PI was denied, the source of the entity's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such denial, as specifically permitted or required by law or regulation.		
	Permits data subjects to update or correct PI: Data subjects are able to update or correct PI held by the entity. The entity provides such updated or corrected information to third parties that were previously provided with the data subject's PI consistent with the entity's objective related to privacy.		Article 16
	Communicates denial of correction requests: Data subjects are informed, in writing, about the reason a request for correction of PI was denied and how they may appeal.		

Disclosure to third parties

PMF ref. #	Components of the PMF	TSC relevant references	GDPR article references
D6.0	Disclosure to third parties	P6.0, *Privacy criteria related to disclosure and notification*	Articles 12, 15, 19, 26, 28, 33, 34, 46, 47, 48, 49
D6.1	The entity discloses PI to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.		
Points of focus	**Communicates privacy policies to third parties:** Privacy policies and specific instructions or requirements for handling PI are communicated to third parties to whom PI is disclosed.		
	Discloses PI only when appropriate: PI is disclosed to third parties only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject, unless a law or regulation specifically requires otherwise.		Articles 19, 48
	Discloses PI only to appropriate third parties: PI is disclosed only to third parties who have agreements with the entity to protect PI in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions or requirements.		
	Discloses information to third parties for new purposes and uses: PI is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of data subjects.		
D6.2	The entity creates and retains a complete, accurate and timely record of authorized disclosures of PI to meet the entity's objectives related to privacy.		
Point of focus	**Creates and retains record of authorized disclosures:** The entity creates and maintains a record of authorized disclosures of PI that is complete, accurate and timely.		Article 19
D6.3	The entity creates and retains a complete, accurate and timely record of detected or reported unauthorized disclosures (including breaches) of PI to meet the entity's objectives related to privacy.		
Point of focus	**Creates and retains record of detected or reported unauthorized disclosures:** The entity creates and maintains a record of detected or reported unauthorized disclosures of PI that is complete, accurate and timely.		Article 33 (5)

PMF ref. #	Components of the PMF	GDPR article references
D6.4	The entity obtains privacy commitments from vendors and other third parties who have access to PI to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	
Point of focus	**Discloses PI only to appropriate third parties:** PI is disclosed only to third parties who have agreements with the entity to protect PI in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions or requirements.	Articles 26 (1), (2), (3); 28 (1), (2), (3), (4), (5), (6), (7), (8), (9); 46 (1), (2), (3); 47 (2); 49 (1), (2), (3)
D6.5	The entity obtains commitments from vendors and other third parties with access to PI to notify the entity in the event of actual or suspected unauthorized disclosures of PI. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.	
Points of focus	**Remediates misuse of PI by third parties:** The entity takes remedial action in response to misuse of PI by a third party to whom the entity has transferred such information.	
	Reports actual or suspected unauthorized disclosures: A process exists for obtaining commitments from vendors and other third parties to report to the entity actual or suspected unauthorized disclosures of PI.	Article 33 (2)
D6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators and others to meet the entity's objectives related to privacy.	
Points of focus	**Remediates misuse of PI by third parties:** The entity takes remedial action in response to misuse of PI by a third party to whom the entity has transferred such information.	
	Provides notice of beaches and incidents: The entity has a process for providing notice of breaches and incidents to affected data subjects, regulators and others to meet the entity's objectives related to privacy.	Articles 12 (1); 33 (1), (2), (3), (4); 34 (1), (2), (3), (4)
D6.7	The entity provides data subjects with an accounting of the PI held and disclosure of the data subjects' PI, upon the data subjects' request, to meet the entity's objectives related to privacy.	
Points of focus	**Identifies types of PI and handling processes:** The types of PI and sensitive PI and the related processes, systems and third parties involved in the handling of such information are identified.	Article 15 (1)
	Captures, Identifies and Communicates Requests for Information: Requests for an accounting of PI held and disclosures of the data subjects' PI are captured, and information related to the requests is identified and communicated to data subjects to meet the entity's objectives related to privacy.	Articles 12 (1), (3); 19

Security for privacy

PMF ref. #	Components of the PMF		TSC relevant references	GDPR article references
S7.0	Security for privacy		N/A (general security criteria)	Articles 5, 24, 25, 30, 32, 35, 45, 46
S7.1	The entity implements logical access security control software, infrastructures, authentication mechanisms and related architectures and security configuration controls over protected information assets to protect them from security incidents and events that might result in unauthorized access, alteration, destruction or disclosure of that information, and to meet the entity's privacy objectives.			
Points of focus		**Identifies and manages the inventory of information assets:** The entity identifies, inventories, validates, classifies and manages information assets.		Article 30 (1), (2), (3), (4), (5)
		Restricts logical and physical access to PI: The entity restricts logical and physical access to its information assets, including computing and network hardware, application systems, data (at-rest, during processing or in transmission), software, administrative authorities, mobile devices, output, and offline system components are restricted through the use of authentication and access control software and rule sets, and access to information assets is logged and monitored based on defined access authorizations.		Articles 25 (1); 32 (1)
		Identifies and authenticates users: Persons, infrastructure, network devices and software are identified and authenticated, and their access privileges are validated prior to granting access to information assets, whether locally or remotely.		Article 32 (1)
		Considers network segmentation: The entity considers and, when deemed necessary, uses network segmentation to restrict access within and between its internal network segments and external networks. Segmentation permits unrelated portions of the entity's information system to be isolated from other network segments.		Article 32 (1)
		Manages points of access: Points of access to the entity's information assets from internal and external users and outside entities and the types of data that flow through the points of access are identified, inventoried and managed. The types of users and the systems authorized to connect to each point of access are identified, authenticated and logged, and their activities within such systems are monitored.		Article 32 (1)
		Restricts access to information assets: The entity uses a combination of controls to restrict access to its information assets including data classification. The entity enforces logical separations of data structures and the segregation of incompatible duties applies device security hardening and security configuration policies, including activating system service restrictions, IP address validation and logical and physical access controls to servers and network device communication ports. The entity also uses updated access protocols to enable and enforce user and system access restrictions, user identification, authentication and logging, and user access behavior monitoring controls. The entity administrates digital certificate software tools to protect user communications and to enforce rules and policies for information asset access.		Articles 5 (1)(f), 32 (1)

PMF ref. #	Components of the PMF	GDPR article references
	Manages identification and authentication: User and system identification and authentication policy and procedure requirements are established, documented, managed, monitored and enforced for users and systems accessing the entity's information, infrastructure platforms and network devices, application systems, data storage systems and utility software.	Article 32 (1)
	Manages credentials for infrastructure and software: The entity has established policies and procedures and technical specifications and requirements for the configuration and credentialing of users and systems prior to granting logical access to information and data about internally and externally managed infrastructure-based platforms, devices and software. The entity's procedures for provisioning and restricting access help make sure that systems and users are registered, authorized, documented and evaluated before access credentials and privileges are established and implemented via the network or from remote access points. User and system authorization and access credentials and privileges are removed and access is disabled when no longer required and when the infrastructure and software are no longer in use. The entity's procedures require that system and user access credentials be periodically revalidated for continued business need.	Articles 5 (1)(f), 32 (1)
Points of focus	**Uses encryption to protect data:** The entity uses data encryption to supplement other measures to protect data in transit and at rest when such protections are deemed appropriate based on the assessed level of risk. The entity administrates, maintains and manages its encryption key management systems and regularly backs up its key stores to help these remain available in the event of a key management system outage or failure.	Article 32 (1)(a)
	Protects encryption keys: Processes are in place to protect public and private encryption keys during generation, storage, use, deactivation and destruction.	Article 32 (1)(a)
	Uses antivirus and anti-malware software: The entity uses antivirus and anti-malware software and requires that it be implemented and maintained on all end-point devices connected to the internal and external networks to provide for the interception, detection and remediation of malware. The entity also requires third-party service organizations to confirm that their users and systems that connect to the entity's internal networks, infrastructure systems, network devices, application systems and data storage devices and information, also have active and currently updated antivirus and anti-malware protections.	Article 32 (1)

PMF ref. #	Components of the PMF		GDPR article references
S7.2	The entity restricts physical access to facilities and protected information assets (e.g., data center facilities, back-up media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.		
Points of focus		**Managing physical access:** The entity has implemented policies and procedures that restrict physical access to the entity's data centers, office spaces, documents, work areas and facilities based on an individual's needs for access, prior authorizations from a facility or system owner, and after the identity of each individual has been established prior to allowing access.	Article 5 (1)(f)
		Removes physical access: Processes are in place to remove physical access to facilities and system resources when an individual no longer requires access.	
		Ongoing physical access monitoring: Processes are in place to periodically evaluate and re-validate (with the appropriate authorities) everyone's need for physical access and to make sure such access is consistent with the entity's business needs and the individual's specific job responsibilities.	
		Internal physical access control: The entity requires individuals to be issued a proximity badge and has implemented proximity control mechanisms that require an individual to authenticate their identity via proximity card reading devices prior to gaining access to internal locations within the entity's data centers, office spaces, document storage locations, work areas and environmental control system locations.	
		Physical protection of information on storage media: The entity has policies and procedures in place that address the physical protection of information and system and data storage devices and removable media. The policies and procedures include the handling and secure operation of such devices, and their removal from service, the removal of information assets residing on such devices and their eventual secured destruction.	
		Identifies environmental threats: As part of the risk assessment process, management identifies environmental threats that could impair the confidentiality, integrity and availability of systems, including threats resulting from adverse weather or the failure of physical access control and environmental control systems, or from electrical discharge, fire and water damage.	Article 32 (1)(b)

PMF ref. #	Components of the PMF		GDPR article references
S7.3	The entity restricts the transmission, movement and removal of information to authorized internal and external users and processes, and protects it during transmission, movement or removal to meet the entity's objectives.		
Points of focus		**Restricts the ability to perform transmission:** Data loss prevention processes and technologies are used to restrict a user or system's ability to exfiltrate protected information, to execute data transmission, move information stored logically or maintained in physical devices, or otherwise modify, view, reproduce or destroy such information.	Articles 45 (1), 46 (1)
		Uses encryption technologies or secure communication channels to protect data: Encryption technologies or secure communication channels are used to protect data in transit and at rest, and communications of such data beyond the entity's established connectivity mechanisms are logical with physical access points.	Article 5 (1)(f)
		Protects end point and mobile devices: Processes are in place to protect endpoint and mobile computing and personal productivity devices (such as laptop and desktop computers, servers, networking and data storage devices, smart phones and tablets) that are used in computing, networking, data storage and processing of the entity's information assets.	
		Protects removable media: Encryption technologies and physical (hardware) device protections are used for peripherals and removable data storage media (such as remote printers that store system-generated data, USB ports, drives, remote USB storage devices and data back-up media), as appropriate.	
S7.4	The entity protects PI, in all forms, against accidental disclosure due to natural disasters and environmental hazards.		
Point of focus		**Continuity of physical and environmental protections:** The entity has established policies and procedures that prevent, detect and react to system outages, incidents and events that disrupt system processing, or results in the loss, accidental disclosure or unauthorized modification of the entity's PI.	Article 32 (2)
S7.5	The entity tests the effectiveness of the key administrative, technical and physical safeguards protecting personal data, periodically and as required by entity policy, or by relevant, applicable laws or regulations.		
Points of focus		**Considers different types of ongoing and separate evaluations:** Management uses a combination of different ongoing and separate evaluations, including system internal and external penetration testing, third-party independent verifications and certifications using established security control frameworks (NIST, COBIT, OWASP, etc.) and vendor and industry-specific, and the entity's own defined technical specifications, security requirements and configuration standards (e.g., performing ISO, PCI or TSP certifications), and internal audit assessments to monitor the effectiveness of required administrative, technical and physical safeguards.	Articles 24 (1), (3); 25 (3); 32 (1)(d), (3); 35 (8)

PMF ref. #	Components of the PMF	GDPR article references
	Implements incident management and recovery testing: Incident management and system recovery testing is performed on a periodic basis to make sure the entity continues to be able to identify, evaluate and respond to critical incidents. Testing includes: 1) the development and use of test scenarios based on the likelihood and magnitude of potential threats and known vulnerabilities; 2) consideration of system components that might impair system and information availability; 3) scenarios that consider the potential for key person availability; and 4) the updating of continuity and resiliency plans, procedures and systems based on test results.	Article 32 (1)(c)
	Implements business continuity plan testing: The entity periodically tests the effectiveness of its business continuity and resiliency plans, procedures and capabilities to make sure that they continue to protect the entity from the adverse effects of unplanned system outages or damages that render systems and information assets unavailable or compromised. Testing includes: 1) the preparation and execution of risk scenario events that consider the likelihood and magnitude of identified threats and known vulnerabilities and system and process weaknesses; 2) the consideration of system components that could impair system processing and information confidentiality, integrity and availability; 3) scenarios that consider the potential impacts to key personnel availability; and 4) the update and revision of plans, processes and systems based on feedback and lessons learned from the results of testing.	Article 32 (1)(c)
	Testing confidentiality, completeness, integrity and availability of systems and back-up data: The continued confidentiality, completeness, integrity and availability of the entity's systems and back-up information is evaluated and confirmed on a periodic basis.	Article 32 (1)(b)

Data integrity and quality

PMF ref. #	Components of the PMF	TSC relevant references	GDPR article references
Q8.0	Data integrity and quality	P7.0, *Privacy criteria related to quality*	Article 5
Q8.1	The entity collects and maintains accurate, reliable, up to date, complete and relevant PI to meet the entity's objectives related to privacy.		
Points of focus	**Communicates to data subjects:** Individuals are informed that they are responsible for providing the entity with accurate and complete PI and for contacting the entity if correction of such information is required.		
	Ensures accuracy and completeness of PI: PI is accurate and complete for the purposes for which it is to be used.		Article 5 (1)(d)
	Ensures relevance of PI: PI is relevant for the purposes for which it is to be used.		

Monitoring and enforcement

PMF ref. #	Components of the PMF	TSC relevant references	GDPR article references
M9.0	Monitoring and enforcement	P8.0, *Privacy criteria related to monitoring and enforcement*	Articles 5, 22, 24, 25, 32, 35, 38
M9.1	The entity implements a process for receiving, addressing, resolving and communicating the resolution of inquiries, complaints and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.		
Points of focus	**Communicates to data subjects:** Data subjects are informed about how to contact the entity with inquiries, complaints and disputes.		Article 38 (4)
	Addresses inquiries, complaints and disputes: A process is in place to address inquiries, complaints and disputes.		Article 22 (3)
	Documents and communicates dispute resolution and recourse: Each complaint is addressed and the resolution is documented and communicated to the individual.		
	Documents and reports compliance review results: Compliance with objectives related to privacy are reviewed and documented and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.		Articles 5 (2); 24 (1), (3); 25 (3); 32 (3); 35 (8), (11)
	Documents and reports instances of noncompliance: Instances of noncompliance with objectives related to privacy are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.		
	Performs ongoing monitoring: Ongoing procedures are performed for monitoring the effectiveness of controls over PI and for taking timely corrective actions when necessary.		

Contributors

This Privacy Management Framework (PMF) was approved by the AICPA Privacy Task Force and AICPA Information Management and Technology Assurance Executive Committee on March 1, 2020. The adoption of the PMF is voluntary.

Information Management and Technology Assurance Executive Committee (2019–2020)

Steven J. Ursillo Jr., CPA, CISA, CISSP, CCSFP (chair)
Partner — Risk Assurance and Advisory
Cherry Bekaert LLP

Vincent Accardi, CPA/CITP, CIPP-E, CISA
Senior Manager — Information Security and Information Technology Governance, Risk and Compliance
PwC

Yuang-Sung Chen, CPA/CITP, CGMA
Professor
North Carolina State University

Steven Konecny, CFE, CISM, CRISC
Partner
Forensic Security Solutions

David A. Kovar, Ph.D.
Interim Chief Executive Officer
Tax Prodigy

Jeffrey Krull, CPA, CISA
Partner
Baker Tilly Virchow Krause, LLP

Gary Lubin, CPA/CITP, CGMA
Investor International Business/Financial Advisor
InRun Capital

Gina Pruitt, CPA/CITP, CISA, CRISC, CHFP, CCSFP, CHCO
Member-in-Charge, Risk Assurance and Advisory Services
KraftCPAs PLLC

John Shamash, CPA/CITP, CA
Chief Financial Officer
Gorski Group

Brian Thomas, CISA, CISSP
Partner in Charge — Advisory Services
Weaver

Amy Vetter, CPA/CITP, CGMA
Chief Executive Officer
The B3 Method® Institute

Torpey White, CPA/CITP, CISA, CGEIT, CGMA
Partner
Wipfli LLP

Privacy Task Force (2019–2020)

Vincent Accardi, CPA/CITP, CIPP-E, CISA (chair)
Senior Manager — Information Security and Information Technology Governance, Risk and Compliance
PwC

Angela Appleby, CPA/CITP, CISA, CISSP, CIA, PCI-QSA, HITRUST CCSFP
Partner
Plante Moran

Nancy Cohen, CPA, CIPP/US
Manager — Data Protection and Privacy Practices
Ernst and Young LLP

David A. Kovar, Ph.D.
Interim Chief Executive Officer
Tax Prodigy

Tom Patterson, CPA, CISA, CGEIT, CRISC
Director, Security Advisory Services
Security Assurance LLC

AICPA staff

Susan C. Allen, CPA/CITP, CGMA
susan.allen@aicpa-cima.com

Appendix A — Glossary of terms

Affiliate — An entity that controls, is controlled by, or is under common control with another entity.

Agreement — An explicit agreement between a data subject who is the legal owner of their personal information (PI) with someone who has a fiduciary or legal duty to the data subject, such as a parent or legal guardian of a minor, or someone who has a legal power of attorney to act in the place of an original data subject.

Anonymize — The removal of any person-related information that could be used to identify a specific individual.

California Consumer Privacy Act (CCPA) — A bill that enhances privacy rights and consumer protection for residents of the state of California. The bill became effective Jan. 1, 2020.

Confidentiality — The protection of non-PI and data from the risk of unauthorized disclosure.

Consent — An agreement executed by an individual on behalf of an entity authorizing them to collect, use and disclose PI under an executed privacy agreement. Such agreements should be explicit but may be implied depending on the jurisdiction in which the entity operates or provides services. Explicit consent is generally given orally (if recorded), electronically and in writing, and is unequivocal and must disclose and reflect the purposes and needs for which the entity seeks the data subject's explicit consent.

Controller — An entity that has taken possession and controls access to a data subject's PI.

Cookies — Pieces of data generated or collected in web browsers or by a web server and stored in either a user's computer or web server and are ready for use by the web application when the user browses the application in the future. This data can then be used by an entity hosting the web server to identify and track the user's browsing history and searches or when the user returns to the website.

Cookies are also designed to help personalize the web content presented to a user of the browser on which the cookies were stored based on prior interests, preferences, searches and the locations where the user logged in. Cookies can be used to offer targeted marketing materials and items of potential interest based on the user's previous internet sessions. Advertisers can use cookies and other tracking methods to analyze user behaviors. When different users use a computer that was previously used by another person, the website may inspect the cookies could execute the new user's session using the wrong user's preferences. For this reason, recent privacy legislation has focused on the collection of a browser's cookies and browsing history and the use of that data by a website's owner, processor, operator or controller.

Data subject — The individual legal person from whom PI is sought, collected, processed, used, controlled and handled by another legal person or entity.

Encryption — The process of transforming information to make it unreadable to anyone except those possessing a special key (to decrypt).

Entity — An organization that collects, uses, retains and discloses PI.

General Data Protection Regulation (GDPR) — A regulation in the European Union (EU) law on data protection and privacy for all individuals within the EU and the European Economic Area (EEA). The regulation is effective as of May 25, 2018.

Health Insurance Portability and Accountability Act (HIPAA) — An act of the U.S. Congress that stipulates how personally identifiable information is to be protected by the health care and health care insurance industries. It was signed into law in 1996.

Individual — The person about whom the PI is being collected (sometimes referred to as the data subject).

Internal (entity) personnel — Employees, sub-contractors, authorized agents and others acting on behalf of the entity, its affiliates and its service providers.

Opting in — PI may not be collected, used, retained and disclosed by the entity without the explicit consent of the individual.

Outsourcing — The use and handling of PI by a third-party service organization engaged by a legal entity or person to provide processes, services or products or to operate a business function on behalf of the legal entity or person.

Personal information (PI) — Information and data that can describe, characterize, identify or otherwise verify an identifiable legal person or a group of people (data subject).

PI lifecycle — The end-to-end process of obtaining agreement (consent), collecting, creating, using, storing and retaining, disclosing, erasing and disposing, masking and anonymizing a legal person's identifying information.

Policy — A written statement that communicates management's intent, objectives, requirements, responsibilities and standards.

Processor — An entity that provides data and information processing services to other legal persons, entities and organizations. A processor entity may be an application, platform, infrastructure, data storage (as a service) organization, or a private or public cloud-providing business entity.

Privacy — The rights and obligations of individuals and organizations concerning the collection, creation, use, retention, disclosure and destruction of PI.

Privacy breach — A data privacy breach occurs when an individual or organization breaks into systems or locations where PI was collected, created, used or stored in an unauthorized manner (without the explicit permission of the data subjects or the entity controlling or processing the data) and causes the data to be disclosed in ways that are not under the entity's policies, applicable laws or regulations.

Privacy program — The organization, people, policies, procedures and preventive and detective controls placed into effect that allow a legal entity to manage and protect the PI collected from data subjects according to its agreements, business needs and applicable laws and regulations.

Purpose — The reason why an entity seeks to collect, use, create, store and disclose the PI of a data subject. The purposes should be explicit, acknowledged by the entity in an agreement with affected data subjects, and the entity should not use the data subject's PI for other purposes not agreed to by the data subject.

Redact — To delete or black out PI or data on a physical document or in a data file. Data masking is a technical form of redaction that helps an entity prevent the unauthorized disclosure of a data subject's PI.

Revocation — A data subject must be allowed to request access to the PI an entity has collected from or holds on their behalf and should be able to revoke their continued permission for the entity's collection, creation, use, processing and retention of a data subject's PI. An entity that seeks to transfer processing and control of a data subject's PI to another legal entity or person remains responsible for notifying affected data subjects of the other processor and controller's roles and for allowing a data subject to revoke their permission to continue to use and hold the data subject's PI.

Sensitive PI — This is PI that requires a higher duty of care when it comes to processing and controlling, for example, for personal health information including known medical or health conditions, financial information, racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, sexual preferences or interests, or information related to prior criminal arrests and convictions.

Third party — This is an entity or service organization that may not be legally controlled by a covered entity but might otherwise be legally affiliated with the covered entity that collects PI. In many cases, affiliated entities are also impacted by and should be covered by the originating covered entity's privacy agreements or by applicable legal statutes.

Worldwide leaders in public and management accounting

Founded by AICPA and CIMA, the Association of International Certified Professional Accountants powers leaders in accounting and finance around the globe

888.777.7077 | aicpa.org/IMTA