NIST's Privacy Framework for Proposed US Federal Privacy Law

The number of cyberbreaches is ever-increasing. According to the *H1 2022 Data Breach Report*, ransomware, malware (destructive software) and phishing caused 87 percent of data compromises in the United States in the first half of 2022.[1] This negatively affected many organizations and the public in general, causing US state governments to respond by enacting new privacy laws. However, the growing complexity and number of US state privacy laws has made it more difficult for enterprises to manage privacy protection. Too many lawyers offer too few timely answers concerning which compliance laws and reports must be monitored and followed, and how much in enterprise investments of time and money to allocate, while ransomware and breaches result in an increasing number of cyberincidents. A call has arisen for a standardized US federal privacy law.

The US Congress has drafted the proposed American Data Privacy and Protection Act (ADPPA)[2] spurred by the growing wave of US state and municipal privacy laws that have left a fragmented compliance landscape for enterprise executives to manage.

The ADPPA contains a private right of action and generally preempts state laws, including comprehensive privacy laws enacted by the US States of California, Colorado, Connecticut, Utah and Virginia. However, it also preserves 16 different categories of state laws, including consumer protection laws of general applicability and data breach notification laws.

The current legislative proposals generally cover:

- Data minimization
- Data processing restrictions
- Privacy by design
- Published privacy policies
- Individual rights and consent
- Children's data
- Third-party data-collecting entities
- Large data holders
- Private right of action
- State preemption

A US federal law could preempt and unify the splintered state privacy regulations, but enterprise executives will also need to unify their cybersecurity and data privacy efforts to gain economies of scale for their enterprise operations and IT resources.

Data protection and data privacy are complex issues with cybersecurity risk represented by deeply intertwined strands. Just as humans cannot function properly without healthy DNA structures, organizations cannot operate without security priorities and privacy policies working jointly to achieve enterprise goals for growth and opportunity.

VALDEZ LADD | CDPSE, CISSP

Is a cofounder of Privacy Test Driver LLC, which strives to keep organizations safe and productive. He has experience in the telecommunications and healthcare industries and is a member of several security organizations, including ISACA®, the International Information System Security Certification Consortium ([ISC]²) and the Information Security System Association (ISSA). He has provided certification security training reviews to ISACA and ISSA members and has presented at multiple ISSA information security conferences.

The meshing of operations, data privacy and enterprise governance can provide new products and services with Pareto efficiency, which includes privacy protection values.

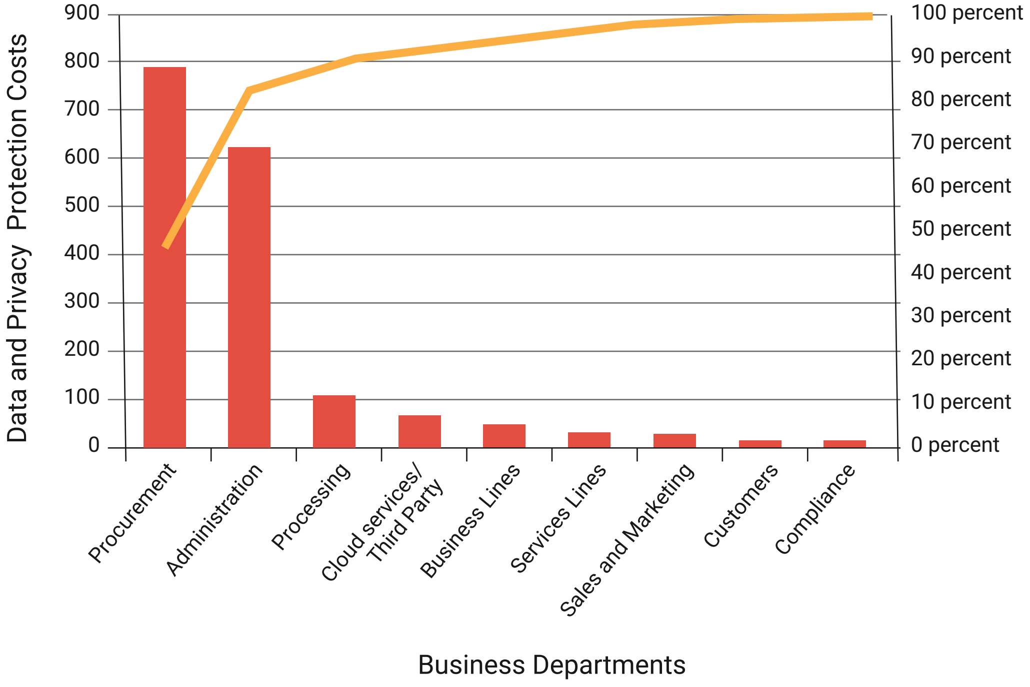
The NIST Privacy Framework

The US National Institute of Standards and Technology (NIST) Privacy Framework[3] is a standalone benchmark framework for privacy awareness and assurance assessments with expert recommendations applicable in both the United States and internationally. Its goal is to introduce an active road map for organizations to embed the best practices of data privacy. Although there are many other frameworks and standards available, such as the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standards ISO/IEC 27018:2019 *Information technology—Security techniques—Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*,[4] ISO/IEC 27701:2019 *Security techniques—Extension to ISO/IEC 27001, ISO/IEC 27002 for Privacy information management—Requirements and guidelines*,[5] and ISO/IEC 31000 *Risk management*,[6] the NIST Privacy Framework is a lighter-weight tool set for privacy analysis. It is a good baseline and can be used as one tool of many for privacy management within the context of the enterprise value stream as the starting point to embed privacy protections, best practices and controls from an organizational perspective.

To begin the privacy discovery process focused on privacy awareness—unlike the privacy assessment of a process, product or individual system, which is done through a privacy impact assessment (PIA) and used in the NIST Privacy Framework—a privacy awareness and readiness (PAR) assessment can be used.[7] This takes an enterprisewide perspective based on business product and business lines throughout the enterprise. The new privacy perspective analysis allows the PAR assessment to be included in the value stream metrics of the operations for the entire enterprise if that scope of work is needed. In addition, the meshing of operations, data privacy and enterprise governance can provide new products and services with Pareto efficiency, which includes privacy protection values (**figure 1**). Pareto efficiency considers the qualitative and quantitative cost analysis of the business product and service flows for production along with real

FIGURE 1

Pareto Efficiency Chart



costs of data privacy protections. Pareto efficiency is achieved when no economic changes can make one business silo or unit better off without making at least one other business silo or unit worse off for the entire enterprise value stream.[8]

Figure 2 illustrates the NIST Privacy Framework's cybersecurity DNA as a starting point.[9]

At its core, the NIST Privacy Framework is a quantitative framework based on the Factor Analysis of Information Risk (FAIR) methodology, which is one of the main tools used for evaluating data privacy risk by NIST. FAIR is a quantitative risk analysis model that describes what risk is, how it works, and how to quantify it.[10]

The NIST Privacy Framework should become the backbone of a well-structured privacy protection, audit and compliance program.

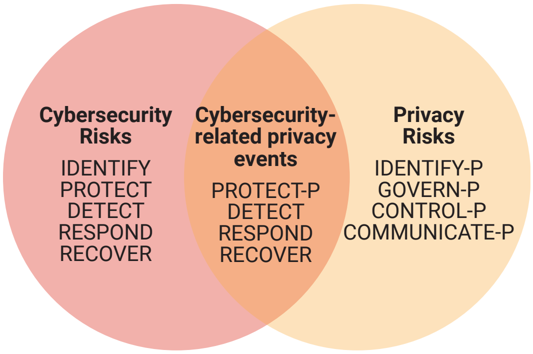
NIST Privacy Framework Components

The NIST Privacy Framework core describes privacy activities and outcomes used to determine how to manage privacy risk. The activities and outcomes are grouped into five functions (**figure 3**).

These five core elements are used to create profiles that show an organization's current and future state of data privacy management maturity. Each profile can show a current state and future goal state of better privacy management efficiency.

FIGURE 2

NIST Privacy Framework Functions



Source: National Institute of Standards and Technology (NIST), *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0*, USA, 16 January 2020, *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf*. Reprinted with permission.

There are four implementation tiers that include additional supporting information.

- **Tier 1: Partial**—Limited awareness, no formalized privacy process, *ad hoc* risk assessment
- **Tier 2: Risk-informed**—Awareness of privacy risk informs the process, but no formal organizationwide privacy policies exist
- **Tier 3: Repeatable**—Formal policies, organizationwide privacy risk management
- **Tier 4: Adaptable**—Continuous privacy improvement, clear relationship between privacy risk and organizational objectives

These tiers should be combined with data security and privacy controls to leverage other data security standards.

FIGURE 3

NIST Privacy Framework Data Security Control Objectives

Controls	Objectives
Identify-P	Discovery, inventory of data assets and assigning of ownership to data
Govern-P	Building and maintaining a secure network and systems
Control-P	Protecting data, including financial and personal information
Communicate-P	Maintaining a vulnerability management program
Protect-P	Implementing multifactor access control measures, regularly monitoring and testing networks, and maintaining an information security and privacy policy

Privacy value stream mapping assists executives in envisioning and prioritizing how business value flows are managed throughout the enterprise.

Within each tier, there are four elements:

1. Privacy risk management process
2. Integrated privacy risk management program
3. Data processing ecosystem relationships
4. Workforce

Although each tier can be assessed independently from the others, it needs to be anchored to the operations and mission of the organization. The specific core functions, tiers and sub-tiers help create an active profile that assists the organization in prioritizing resources for managing privacy risk.

The NIST Privacy Framework should become the backbone of a well-structured privacy protection, audit and compliance program. Having the ability to implement privacy controls and then map those to current state or province laws is useful and adds enterprise value to the chief information officer (CIO), chief security officer (CSO) or senior legal counsel as it reveals the current state of cybersecurity and privacy risk.

Modern organizations want well-synchronized operations that will increase their capabilities to meet the demands of evolving, borderless marketplaces. This requires that enterprise audit, cybersecurity, development, operations, marketing and finance teams become more engaged in a structured effort to communicate privacy issues with senior management to produce working solutions. Operational privacy protection best practices include:

- Create privacy-by-design conforming products, services and processes by embedding data protection throughout the value streams.
- Recognize the benefits of emerging technologies while respecting customer privacy.
- Protect data integrity.
- Establish privacy practices for data security and privacy controls for areas such as data minimization, zero trust networking and encryption.

Although the NIST Privacy Framework is a good tool, it must be supplemented to account for the complexity of data and organizational management in the modern digital enterprise. Communications between organizational lines (services and products) is required to be effective.

SIPOC Model

Conway's Law states that "Organizations, who design systems, are constrained to produce designs which are copies of the communication structures of these organizations."[11]

This often leads to organizational silos, constrained communications and value flows that may contain unmanaged dark data. Privacy and security risk often follow the social boundaries of the enterprise's informal operational structures and hierarchies that produce barriers to effective data privacy risk management programs. These barriers inhibit scalability for cost efficiency.

Executives have the responsibility to steer mission priorities, decide risk tolerance, establish organizational privacy values, budget, and determine acceptable privacy risk decisions.

An excellent tool senior management can use to navigate this vision curve is the suppliers, inputs, process, outputs and customers (SIPOC) model, which is used to analyze operational processes (**figure 4**).[12] SIPOC analysis helps describe the value-creation dynamics of work groups, organizations and networks engaging in both tangible and intangible value creation.[13] This creates a holistic view that breaks down and simplifies organizational complexity by layering and abstracting organizational structures, capabilities and management into consistent product and service value streams.

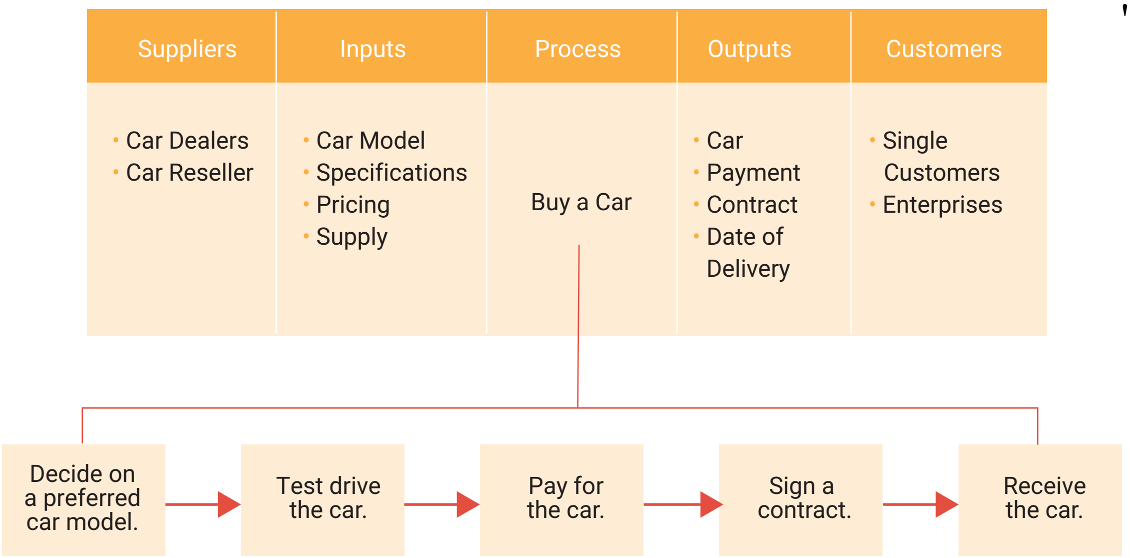
The SIPOC model allows an organization to view its value streams within each operational unit's specializations. This yields insights on data governance and uncovers hidden obstacles. The SIPOC model complements the NIST Privacy Framework by visually grounding it within the organization's functions. These visual insights suggest trade-offs, which may include creating the proper mixture of reliability, security, usability, performance and functionality requirements of the enterprise value streams.

LOOKING FOR MORE?

- Read *Privacy by Design or Default: A Primer.* *www.isaca.org/Privacy-by-Design*
- Learn more about, discuss and collaborate on privacy in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

FIGURE 4

Example of a Car Purchase Using SIPOC



Suppliers	Inputs	Process	Outputs	Customers
• Car Dealers • Car Reseller	• Car Model • Specifications • Pricing • Supply	Buy a Car	• Car • Payment • Contract • Date of Delivery	• Single Customers • Enterprises

Source: Wondershare EdrawMax, "Free Editable SIPOC Diagram Examples," *https://www.edrawmax.com/article/sipoc-diagram-examples.html*. Reprinted with permission.

Privacy Value Stream

This journey begins by auditing and analyzing data governance processes for:

- Data discovery
- Data protection
- Identity and access management (IAM)

These form the basis for the creation of individually specific data security and data privacy protection measures, processes and audits for enhancing the privacy value stream of each organization. No two organzations are managed the same. Each organization metabolizes information for its value creation differently. Therefore, no one-size-fits-all solution will work for privacy effectiveness.

The next steps are to move to more specific data security and data privacy protection measures. Data discovery, data protection, and identity and access management form the operational data security control objectives that must be included within an effective data privacy protection operations program. The merger of these elements supports digital trust.

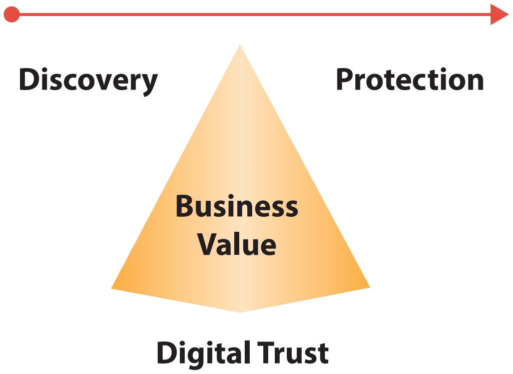
Data protection and data privacy are complex. Although the NIST Privacy Framework is a good starting point for a program for data privacy and compliance in the US and internationally, it still must be combined with other tool sets to incorporate operational, technical and managerial oversight into a comprehensive program that meets the executive mission objectives of the enterprise.

Privacy value stream mapping assists executives in envisioning and prioritizing how business value flows are managed throughout the enterprise (**figure 5**). This improves visibility and insights into operations per business line (products and services) that would not otherwise be identified or held accountable. This allows data security, data privacy protection and digital trustworthiness to be measured, managed and magnified for business success.

Once an enterprise has an established privacy program primarily focused on maintaining

FIGURE 5

Privacy Value Stream Triangle



privacy protection that meets or exceeds the legal compliance requirements, then new opportunities should emerge. It is likely that the enterprise will find less risk, lower operational costs and greater transparency. Some benefits may include paying lower cyberinsurance premiums, better business-to-business (B2B) growth, and growth in customer trust. These advantages allow enterprises to focus on managing privacy protection and compliance as part of their enterprise market growth goals and should give them a competitive advantage.

Executives must continually make critical decisions about resource allocations and budgets in the face of market competition and cybersecurity threats. Senior executives must orchestrate a common agreement on shared business goals to support the enterprise mission.

Business engineering is typically filled with trade-offs.[14]

Conclusion

Governments around the world are enacting data security and data privacy rules and regulations at an increasing pace that is forcing enterprises to react, respond and realign their businesses to meet these challenges.

Specifically, US federal and state data privacy laws, such as the draft for the ADPPA, are complicated and difficult to manage for enterprise compliance professionals. The NIST Privacy Framework, along with SIPOC and other tools, allows organizations to better navigate these requirements. Integrating process and value streams can greatly increase enterprise risk management worthiness.

These tools help determine the best action by forging and enabling security and privacy risk management programs that integrate with value streams. Ultimately, customers receive value-added products and services backed by quality and respected privacy.

Endnotes

1. Identity Theft Resource Center, *H1 2022 Data Breach Analysis*, USA, 13 July 2022, *https://www.idtheftcenter.org/post/h1-2022-data-breach-report-shows-decrease-in-compromises-victim-rates/*
2. Gaffney, J.; E. N. Holmes; C. D. Linebaugh; *Overview of the American Data Privacy and Protection Act*, H.R. 8152, Congressional Research Service, USA, 31 August 2022, *https://crsreports.congress.gov/product/pdf/LSB/LSB10776*
3. National Institute of Standards and Technology (NIST), *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*, Version 1.0, USA, 16 January 2020, *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf*
4. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27018:2019 *Information technology—Security techniques—Code of practice for protection of personally identifiable Information (PII) in public clouds acting as PII processors*, Switzerland, 2019, *https://www.iso.org/standard/76559.html*
5. International Organization for Standardization, International Electrotechnical Commission, ISO/IEC 27701:2019 *Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy information management—Requirements and guidelines*, Switzerland, 2019, *https://www.iso.org/standard/71670.html*
6. International Organization for Standardization, International Electrotechnical Commission, ISO/IEC 31000 *Risk management*, Switzerland, *https://www.iso.org/iso-31000-risk-management.html*
7. Dennedy, M.; J. Fox; T. Finneran; *The Privacy Engineer's Manifesto: Getting From Policy to Code to QA to Value,* Apress Open, USA, 2014
8. Investopedia, "Pareto Efficiency Examples and Production Possibility Frontier," 20 September 2022, *https://www.investopedia.com/terms/p/pareto-efficiency.asp*
9. *Op cit* NIST
10. FAIR Institute, "What Is the FAIR Institute?" USA, *https://www.fairinstitute.org*
11. Conway, M. E.; "How Do Committees Invent?" *Damnation*, April 1968, *http://www.melconway.com/Home/Committees_Paper.html*
12. Schuchart, W.; "SIPOC Diagram (Suppliers, Inputs, Process, Outputs, Customers)," *TechTarget*, August 2019, *https://www.techtarget.com/searchcio/definition/SIPOC-diagram-suppliers-inputs-process-outputs-customers*
13. Allee, V.; "Value Network Analysis and Value Conversion of Tangible and Intangible Assets," *Journal of Intellectual Capital*, vol. 9, iss. 1, 2008, *https://citeseerx.ist.psu.edu/viewdoc/*
14. Cavoukian, A.; *Privacy by Design: The Seven Foundational Principles*, Canada, 2011, *https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf*