Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management

Introduction

The objective for this companion Roadmap to the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Privacy Framework or Framework) is to support continued collaboration between NIST and stakeholders from across government, academia, and industry on privacy risk management. It discusses priority areas that pose challenges to organizations in achieving their privacy objectives. These important, evolving areas require continued focus or further research and development to advance the evolution of the Privacy Framework; promote a well-functioning data processing ecosystem; and expand the body of standards, guidance, practices, and tools supporting privacy risk management. While this list is not intended to be exhaustive, these are important topics based on input and feedback received from stakeholders throughout the Framework development process.

Areas for Development, Alignment, and Collaboration

The following priority areas describe key challenges and some initial activities that can be undertaken to address them. While guidance, standards, practices, and tools exist for some areas, they need to become more mature, available, or widely adopted. Some areas reflect needs directly related to outcomes in the Framework Core (e.g., where a Subcategory lacks informative references). Progress in these areas may feed into future updates to the Framework or result in resources that can be shared in the Privacy Framework Resource Repository.

1. Privacy Risk Assessment

Privacy risk assessment is a process for identifying and evaluating privacy risks, which organizations can use to build customer trust by developing more effective solutions to protecting individuals' privacy when designing or deploying systems, products, and services that process data. This process can also help organizations to bring privacy into parity with their broader portfolio of enterprise risks, driving development of a more robust and comprehensive enterprise risk management approach to promote better decision-making and resource allocation.

In the cybersecurity domain, risk assessment is relatively well established, with a commonly recognized risk model for analysis using the factors of likelihood, vulnerability, threat, and impact.[1] Organizations have at their disposal a substantial body of both public- and private-sector guidance and tools to support cybersecurity risk assessment. This wealth of resources does not yet exist in the privacy domain.[2] The privacy domain lacks development and uptake of uniform concepts of privacy risk assessment, including specific risk factors, as well as more in-depth guidance and tools for assessing privacy risks. As a result, organizations find it challenging to integrate privacy risk assessment into their risk management approaches, assess and measure impacts to individuals, and reflect the impacts to individuals within the organization in actionable ways. In an effort to advance the discipline, the Privacy

[1] NIST Special Publication 800-30, rev 1, *Guide for Conducting Risk Assessments*.
[2] NIST *Summary Analysis of the Responses to the NIST Privacy Framework Request for Information*.

Framework's Risk Assessment Category (ID.RA-P) includes NIST's proposed privacy risk factors (i.e., likelihood, problematic data action, and impact) but NIST recognizes more work is needed to reach a common privacy risk model and more effective privacy risk assessment practices.

Priority activities include:

- workshops or roundtables to further develop concepts of privacy risk assessment;
- development of more in-depth guidance and tools for privacy risk assessment and an integrated approach with cybersecurity guidance; and,
- collaboration and engagement with stakeholders in integrating privacy into enterprise risk management guidance.

2. Mechanisms to Provide Confidence

Organizations can use mechanisms to provide confidence to show that a system, product, or service meets specified requirements. These mechanisms can include audits, assessments and evaluations, and formal conformity assessment activities such as inspection, testing, supplier declaration, or certification. Effective confidence mechanisms provide the needed level of assurance, are efficient, drive improvement, and have a sustainable and scalable business case. An organization can use the output of these mechanisms to enhance its understanding of its Framework Profile implementation and benchmark the effectiveness of its privacy protections.

The privacy domain generally lacks confidence mechanisms, posing a challenge to organizations in demonstrating the effectiveness of privacy protections. More research is needed to understand organizations' challenges and needs with respect to confidence mechanisms for privacy. Resources in the cybersecurity domain could serve as models of what could be developed in the privacy domain. For example, the Baldridge Cybersecurity Excellence Builder is a self-assessment tool to help organizations better understand the effectiveness of their cybersecurity risk management efforts and identify improvement opportunities in the context of their overall organizational performance.[3] While NIST does not endorse any commercial approach, NIST does encourage and support a diverse, market-based set of approaches to instill confidence.

Priority activities include:

- engagement with organizations on framework implementation to learn about their challenges and needs regarding confidence mechanisms, and
- collaboration with stakeholders, including in standards development organizations, to develop standards or guidance on assessment procedures or criteria.

3. Emerging Technologies

A key challenge for the privacy field has been determining how to design systems, products, and services that protect individuals' privacy in an increasingly connected world. While emerging technologies such as Internet of Things (IoT) and artificial intelligence (AI) are driving innovation, economic value, and improvement in social services, they also can amplify the complexity of the data processing ecosystem. For example:

[3] See https://www.nist.gov/cyberframework/assessment-auditing-resources.

- the types of capabilities that may or may not be designed into IoT devices can affect how individuals or organizations using those devices are able to manage privacy risk;
- decentralized data processing can involve various parties that are not contractually bound to each other, challenging traditional accountability mechanisms;
- the volume and nature of decentralized or automated data processing could make it more difficult for individuals to understand how their data is processed and to engage in management of the processing, including obtaining redress to rectify problems; and
- AI systems and automated decision-making create concerns about fair treatment of individuals.

There is a need for research to underpin guidance, standards, practices, and related tools for managing these complexities.

Priority activities include:

- promoting research into the fundamentals that underpin the ability of organizations to understand and manage the privacy risks arising from emerging technologies such as better understanding of concepts such as bias and fairness and how to measure them; and
- the development and integration of privacy guidance into IoT or AI guidance, tools, frameworks, and standards.

4. De-Identification Techniques and Re-identification Risks

NIST describes de-identification as a technique or process applied to a dataset with the goal of preventing or limiting certain types of privacy risks to individuals, protected groups, and establishments, while still allowing for the production of aggregate statistics. This broad scope includes data masking, noise-introducing techniques such as differential privacy, and the creation of synthetic datasets that are based on privacy-preserving models.[4] In appropriate contexts, such techniques can be useful to organizations in mitigating privacy risks. While guidance, standards, practices, and tools are beginning to be developed for de-identification, more work is needed to increase their market-readiness and assist organizations with implementation.

Some level of re-identification risk remains even after the application of de-identification techniques. These risks may arise from different sources such as the unanticipated combination of datasets and the use of emerging technologies such as IoT and AI. Further work is needed to promote awareness, measurement, and mitigation of re-identification risks.

Priority activities include:

- convening stakeholders, including in online forums, to develop and improve upon de-identification tools and sharing practices for understanding and managing re-identification risks; and
- collaboration with stakeholders, including in standards development organizations, to develop standards, guidance, and tools around de-identification techniques and managing re-identification risks.

[4] NIST Privacy Engineering Collaboration Space, https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/introduction.

5. Inventory and Mapping

Inventorying data and the circumstances under which data are processed can help an organization to identify and prioritize privacy risks. Creating data maps can be useful in illustrating data processing and individuals' interactions with systems, products, and services. The Privacy Framework includes outcomes supporting such activities in the Inventory and Mapping Category (ID.IM-P), but in an increasingly connected environment with large volumes of data, as well as different types of data (e.g. structured, unstructured), conducting data inventory and mapping activities at an appropriate level of detail can be a daunting task for organizations. More guidance, best practices, and automation in tools for cost-effective data inventorying and mapping is needed to better support organizations' privacy risk management practices.

Priority activities include:

- engagement with stakeholders to learn about their challenges and needs regarding data inventorying and mapping; and
- collaboration with stakeholders, including in standards development organizations, to develop standards, guidance, and tools for data inventorying and mapping.

6. Technical Standards

While there has been an increased focus on the development of international, consensus-based privacy standards, many emerging standards are management system standards focused on processes. There are fewer privacy-related technical and testing methodology standards under development. Technical standards are needed for organizations to achieve the objectives laid out in management system standards. For instance, there are some standards on de-identification, which provide a taxonomy and decision-making framework around which approaches to consider for de-identification, and the terminology to use. However, standards for technical aspects of de-identification, such as defining r-value or defining algorithms for differential privacy in specific contexts could advance the effectiveness of these privacy risk mitigation techniques. Technical standards could also be helpful to organizations in achieving outcomes in the Control Function related to accessing data for various data processing management purposes. These standards could help to improve organizations' capabilities for locating data to better respond to individuals' data management requests. Standardized data formats could support the use of AI technologies to protect privacy such as the development of automated personal assistants. Testing methodology standards can bolster the efficacy of privacy protections. For instance, they provide a way for auditors to test against de-identification algorithms and ensure that data is de-identified to the extent expected.

Priority activities include:

- convening stakeholders to gather information about and identify priority topics where standardization is needed; and,
- engagement with stakeholders, including in standards development organizations, to continue advancing technical and assessment standards that support privacy engineering.

7. Privacy Workforce

The benefits of using the Privacy Framework will be enhanced if organizations have a broader pool of skilled and knowledgeable privacy professionals from which to build their workforce. For example, the Privacy Framework describes the workforce element at Implementation Tier 4 as having specialized privacy skillsets throughout the organizational structure. The demand for such a workforce is currently outpacing the supply. NIST has efforts underway through its National Initiative for Cybersecurity

Education (NICE) Program to address cybersecurity workforce needs which could be leveraged to manage the overlap between privacy risks and cybersecurity risks. However, good cybersecurity does not address all of privacy risk; accordingly, guidance and documentation designed specifically for cybersecurity will not address the full scope of privacy risk.

Further development of a knowledgeable and skilled privacy workforce (to include privacy practitioners and other personnel whose duties require an understanding of privacy risks) is necessary to support organizations in better protecting individuals' privacy while optimizing beneficial uses of data. This development begins with a need for a common taxonomy to categorize and describe a privacy workforce, including identification of privacy work roles; the discrete tasks performed by staff within those roles; and the knowledge, skills, and abilities needed to complete the tasks successfully.

Priority activities include:

- Engagement with stakeholders, including professional associations, academia, and the public sector on privacy workforce and education challenges and needs; and
- coordination with the NIST NICE Program on outreach and mechanisms to support the development of a collaborative privacy and cybersecurity workforce.

8. International and Regulatory Aspects, Impacts and Alignment

Globalization and advances in technology have driven unprecedented increases in innovation, competitiveness, and economic growth. Many governments – at the international, federal, and state/local level – are proposing and enacting strategies, policies, laws, and regulations to optimize beneficial uses of technology while minimizing adverse societal effects. Because many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, these requirements are affecting, or may affect, how organizations operate, conduct business, and develop new products and services. Diverse or specialized requirements can impede interoperability, result in duplication, hinder innovation, and have unintended consequences on privacy. In turn, this can significantly reduce the availability and use of innovative technologies in all industries and hamper the ability of organizations to operate globally and to effectively manage new and evolving risks.

Because the Privacy Framework is consistent with globally accepted standards, guidelines and practices, organizations domiciled inside and outside of the United States can use the Framework to efficiently operate globally and manage new and evolving risks. Conversely, broad use of the Framework will serve as a model approach to strengthening privacy risk management, while discouraging a balkanization caused from unique requirements that hamper interoperability and innovation, and limit the efficient and effective use of resources.

Priority activities include:

- direct engagement with governments and entities to explain the Framework and seek alignment of approaches when possible;
- coordination with federal agency partners to ensure full awareness with their stakeholder community;
- work with industry stakeholders to support their international engagement; and
- information exchange and work with standards development organizations, industry, and sectors to ensure the Privacy Framework remains aligned and compatible with existing and developing standards and practices.