

Ready, Set, Update! Privacy Framework 1.1 + Data Governance and Management Profile Workshop Summary Report

June 25 – 26, 2024
Washington, D.C. and Virtual

On June 25th – 26th, 2024, the National Institute of Standards and Technology (NIST) Privacy Engineering Program (PEP) held a hybrid public workshop, *Ready, Set, Update! Privacy Framework 1.1 + Data Governance and Management Profile Workshop*.¹ The workshop provided NIST with feedback on updating the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Privacy Framework), Version 1.0 and the development of a joint NIST Frameworks Data Governance and Management (DGM) Profile.² June 25th began with a hybrid plenary session at the Herbert C. Hoover Building in Washington, D.C., followed by breakout sessions where both in-person and online stakeholders shared their perspectives about challenges, needs, and opportunities for these new resources.³ Participation for June 26th was virtual only, allowing a final opportunity for stakeholders to participate in the breakout sessions. The plenary was recorded; however, the breakout sessions were conducted under the Chatham House Rule and were not.⁴

Participants from industry, public sector, academia, and civil society attended the workshop. Attendees represented numerous sectors, including financial, information technology, education, energy, government, and healthcare. Participants also represented a mixture of work roles, including privacy, security, risk management, and compliance, ranging from executives to technical specialists. A total of 80 participants attended the workshop in-person. The livestream webcast of the plenary sessions had a total of 1,337 viewers. Attendee numbers for the breakout sessions were as follows:

- For the Privacy Framework 1.1 Update breakout session #1, there were 30 in-person attendees and 321 online attendees.
- For the Privacy Framework 1.1 Update breakout session #2, there were 25 in-person attendees and 87 online attendees.
- For the Privacy Framework 1.1 Update breakout session #3 (virtual only), there were 137 attendees.
- For the DGM Profile breakout session #1, there were 25 in-person attendees and 96 online attendees.
- For the DGM Profile breakout session #2, there were 20 in-person attendees and 148 online attendees.
- For the DGM Profile breakout session #3 (virtual-only), there were 107 attendees.

Plenary Overview

Opening remarks were given by Kevin Stine, the Director of the Information Technology Laboratory at NIST. These remarks provided participants with background information on the Privacy Framework 1.1, the DGM Profile development process, and what to expect throughout the workshop. This was followed by a fireside chat, “Charting the Course: Navigating Tech Challenges with NIST Resources,” featuring

¹ See <https://www.nist.gov/news-events/events/2024/06/ready-set-update-privacy-framework-11-data-governance-and-management>.

² See <https://doi.org/10.6028/NIST.CSWP.01162020> and <https://www.nist.gov/blogs/cybersecurity-insights/new-year-new-initiatives-nist-privacy-framework>.

³ See plenary recording at https://www.youtube.com/watch?v=sWEV5E1CK_M.

⁴ See plenary recording at https://www.youtube.com/watch?v=sWEV5E1CK_M.

Cameron Kerry, the Ann R. and Andrew H. Tisch Distinguished Visiting Fellow – Governance Studies with the Center for Technology Innovation at Brookings Institution. Mr. Kerry discussed the challenges that have emerged in the privacy and cybersecurity landscape over the last ten years and emphasized there is not a “one-size-fits-all” solution for the risks associated with how data are used and collected by organizations. Three panels completed the plenary:⁵

- Pardon Our Dust: NIST Privacy Framework 1.1 Update
- NISTifying Data Governance: Developing a Joint NIST Frameworks Data Governance and Management Profile
- NIST Review of Workshop Concepts

The Privacy Framework 1.1 Update panel examined how processing data has evolved over the years and noted that organizations are relying on the Privacy Framework and CSF to help assess risks in their programs. The DGM Profile panel stressed the importance of intention and seeing the overall vision of data risk management to reduce potential silos from forming within organizations, as well as discussions around common definitions and methodology to help reduce human error. The last panel, the NIST Review of Workshop Concepts, explained the workshop goals and encouraged feedback from attendees to better understand what stakeholders want from a Privacy Framework update and gain insight on how organizations could use the DGM Profile.

General Workshop Themes

Prior to the workshop, NIST released concept papers for the Privacy Framework 1.1 update and the DGM Profile development for feedback to inform the initial public drafts (IPD) of the Privacy Framework 1.1 update and the DGM Profile.⁶ NIST also released a draft crosswalk between the NIST Cybersecurity Framework (CSF) Version 1.1 and 2.0 and the Privacy Framework Version 1.0.⁷ During the breakout sessions, participants engaged in interactive facilitated discussions. The following major themes emerged from these discussions.

Privacy Framework 1.1 Update Themes

Preserving the Privacy Framework’s Flexible, Technology-Neutral Approach

Participants showed strong support for maintaining the Privacy Framework’s flexible, law, sector, and technology-neutral approach to privacy risk management. For example:

- Many participants noted that keeping the Framework flexible allows for a range of uses, from privacy program communication and advocacy with organizational leaders to detailed privacy program assessment or creation from the ground up. Some also expressed that flexibility supports organizations tailoring the Framework to their specific needs.
- Several participants signaled a need for education and training on the Privacy Framework to help users understand its flexible, risk-based approach, suggesting that implementation examples like those within the CSF 2.0 would be a helpful way to highlight potential use cases.

⁵ See the agenda at the bottom of the page on <https://www.nist.gov/news-events/events/2024/06/ready-set-update-privacy-framework-11-data-governance-and-management>.

⁶ See <https://www.nist.gov/document/pf-11-concept-paper> and <https://www.nist.gov/document/dgm-profile-concept-paper>.

⁷ The draft crosswalk can be found at <https://www.nist.gov/document/csf-11-20-pf-10-crosswalkdraft>. CSF 2.0 can be found at <https://doi.org/10.6028/NIST.CSWP.29>.

- Some participants noted that implementation examples will need to be compatible with and complementary to the Privacy Workforce Taxonomy that NIST is working on in parallel to the Privacy Framework 1.1 update.
- Participants generally agreed that artificial intelligence (AI) was one of many new technologies that organizations are deploying, and, therefore, AI and other technologies should be left out of an update to the technology-neutral Privacy Framework.
 - Many participants noted that the NIST AI Risk Management Framework (RMF) could serve as the key resource for AI risk management, and that the DGM Profile could play an important role in illustrating how the Privacy Framework and AI RMF can be used together.⁸
 - Some participants, however, desired additional AI-related outcomes and activities in the Privacy Framework Core.

Privacy Framework Alignment with Cybersecurity Framework, Version 2.0

There was broad support among participants for following the principles NIST proposed in the Privacy Framework 1.1 concept paper.⁹ For example:

- Participants generally supported close alignment between the CSF and the Privacy Framework, except when there was a functional privacy reason not to do so.
 - Some participants noted that the Privacy Framework is often used in isolation within an organization or a function within an organization.
 - Many participants agreed that for the Privacy Framework, NIST should prioritize the needs of privacy programs over strict alignment with the CSF.
 - Participants broadly agreed that NIST should follow the Privacy Framework, Version 1.0 approach and replicate the CSF 2.0's Protect Function where practicable and adapt outcomes where applicable to privacy risk management. However, some participants supported removal of the Protect-P Function, expressing that it is redundant to the CSF Protect Function.
- There was broad consensus that the Privacy Framework should be structured to be a standalone framework that can address the needs of a privacy program, while also maximizing compatibility with the CSF for joint use where applicable or necessary.
- Some participants disagreed on privacy program needs. For example:
 - Some participants argued that the CSF 2.0 Oversight Category was unnecessary to include in the Privacy Framework update, given the existence of the Monitoring and Review Category.
 - Others strongly supported the inclusion of an Oversight Category, stating that this would be helpful for those who need to understand the technology side of privacy. Additionally, some stated that an Oversight Category could list the controls one would look for in NIST Special Publication 800-53 Revision 5 as this would be useful for privacy programs.¹⁰

Terms and Definitions

Participants broadly agreed that the Privacy Framework should use language and concepts that are central for privacy professionals. These language choices were highlighted as being particularly important in the overlap between privacy and cybersecurity risk management. For example:

⁸ See <https://doi.org/10.6028/NIST.AI.100-1>.

⁹ See <https://www.nist.gov/document/pf-11-concept-paper>.

¹⁰ See <https://doi.org/10.6028/NIST.SP.800-53r5>.

- Participants generally agreed that NIST should seek alignment of content between the CSF and the Privacy Framework but noted that collaboration challenges between privacy and cybersecurity are easier to navigate when privacy terminology and concepts are clear and understandable.
- Some participants disagreed about the extent to which Privacy Framework terms needed further clarification. For example:
 - Some participants thought that “Data Processing Lifecycle” may be a better term than “Data Processing Ecosystem”, stating that the term “ecosystem” seemed more technology-focused.
 - Other participants stated that “ecosystem” is a good term because it implies inclusion of all aspects of data processing and mentioned that changing the term may cause confusion.
- Some participants expressed concerns about aligning too closely with the CSF if terms are not tailored to privacy.
 - Some participants felt that privacy and cybersecurity are often thought of as the same thing and that privacy needs to stand on its own to address privacy risks.

DGM Profile Themes

Data Governance Shared Challenges

Participants found that there are widely shared challenges for organizations when it comes to data governance and management.

- The state of organizational data governance varied among participants. Most participants had organization-created data governance processes in place, although some organizations lacked consistency with ad hoc processes. A few organizations did not have a data governance program at all.
- Participants shared many data governance challenges, regardless of the maturity of their data governance programs.
 - Challenges mentioned by participants included unclear definitions of data governance and personnel obstacles.
 - The top governance challenges that participants faced were lack of program structure, siloing or poor cross-functional integration, and unclear roles and responsibilities.

Value of the DGM Profile to Address Shared Challenges

Panelists in the plenary highlighted that there is no “one-size-fits-all” solution to data governance.

Participants in both the plenary and DGM Profile breakout sessions agreed that the DGM Profile could provide a flexible tool to help organizations meet their data governance challenges in a manner tailored to their unique needs. For example:

- Some participants noted that the DGM Profile could help provide much needed consistency around what data governance is.
 - Some participants thought that the DGM Profile could help their organization with guidance and implementation strategies, as well as connecting data governance with other activities within their organization.
- Some participants thought the DGM Profile could be a reference and education tool, as well as provide a better understanding of the NIST frameworks.

- Other participants noted that the DGM Profile could assist with additional important challenges that organizations face, such as cross-functional coordination, and offer guidelines on data governance roles and responsibilities.
- Some participants hoped that the DGM Profile could provide a common taxonomy of terms for data governance and management.

NIST's Approach to the DGM Profile

Although there was not complete consensus, there was broad participant support for the concept paper approach, including general agreement that NIST's four proposed data governance objectives are relevant.¹¹

- Some participants hoped to gain a better understanding of how to use the NIST Privacy Framework, CSF, and AI RMF together, noting that the DGM Profile's matrix approach could help provide this guidance.
- Some participants thought the concept paper approach needed more clarity and explanation around the concept and how this resource would be implemented within an organization.
- Other participants suggested that transparency or data explainability needed to be addressed more clearly within the DGM Profile.

Next Steps

NIST will consider the feedback it received throughout the workshop and use this information to develop the initial public drafts of the Privacy Framework, Version 1.1 and the DGM Profile. Given the DGM Profile's dependency on the Privacy Framework 1.1 update, there may be a decoupling of the timelines for these resources. NIST intends to provide additional opportunities for stakeholder engagement in the months ahead. Any updates to the development schedule can be found on the New Projects web page.¹²

For more information about these ongoing projects, email privacyframework@nist.gov.

¹¹ See <https://www.nist.gov/document/dgm-profile-concept-paper>.

¹² See <https://www.nist.gov/privacy-framework/new-projects>.