NAVEX GLOBAL®

WHITEPAPER

4 Things to Know About Updated NIST 800-53 Standards

In September 2020 the National Institute of Standards and Technology (NIST) unveiled the fifth version of its cybersecurity standard formally known as SP 800-53, "Security and Privacy Controls for Information Systems and Organizations."

Don't let the "Version 5" part of the standard fool you. Previous incarnations of 800-53 had been the cybersecurity framework required to do business with U.S. government agencies. Version 5 is a profound departure from that idea — it's meant to be a standard that **all** organizations should embrace, regardless of whether they are U.S. government contractors.

Version 5 is a significant overhaul of 800-53 in several ways. It will force businesses to pay more heed to their own supply chains, but also give businesses more freedom to design security and vendor risk management systems that make the most sense for their operations.

At a practical level, 800-53 is also something businesses should embrace promptly. Consumer privacy laws are proliferating worldwide. The pandemic and our mass migration to remote work spawned a host of new security threats. The federal government and corporate customers alike expect their suppliers to achieve high security standards. So the urgency to implement Version 5 is real.

How should businesses approach compliance with 800-53's latest version? Let's consider the issues.

WHAT IS NIST TRYING TO DO WITH VERSION 5?

Version 5 tries to thread a delicate needle: imposing more accountability for privacy and cybersecurity across an organization's operations (including down into the supply chain); while being less prescriptive in how risk and compliance teams should achieve that stronger security posture.

To achieve those goals, NIST essentially disassembled previous versions of 800-53 and rebuilt the entire framework. NIST itself described Version 5 as a "complete renovation, addressing both structural issues and technical content." Its major reforms include:

- **Privacy concerns woven into the whole framework.** Previous versions of 800-53 relegated privacy controls into an appendix. Version 5 now has 86 privacy controls, including 26 stand-alone privacy controls and another 60 integrated into security controls.
- **Greater emphasis on supply chain issues.** Version 5 establishes a new control family dedicated to supply chain risk management (the "SR" family) and integrates supply chain management issues into other controls. The controls are meant to extend security compliance even throughout a global supply chain. We should also note that 800-53 defines

"supplier" broadly, to include software-as-a-service (SaaS) vendors, consultants, outsourcing partners, and the like. Any party that provides any good or service to your business counts as a supplier.

- **More discretion in choosing controls.** Version 5 includes a consolidated catalog of controls, so that multiple groups within your enterprise — security or privacy specialists, software developers, enterprise architects, and business-unit operators — can review and select specific controls that meet their needs. The catalog can also foster more cooperation across the enterprise (especially between the security team and operating units in the First Line of Defense) to develop policies and procedures.
- **Making controls outcome-based.** Version 5 now focuses more on the protection delivered by controls, rather than the specific structure those controls should have. This will allow an organization using 800-53 to be more agile with updates to its controls, so the business can keep pace with constantly evolving threats.

In other words, 800-53 Version 5 is a security framework fit for the modern business world — one with long, complex supply chains; rapidly evolving regulatory compliance burdens; and customers who demand effective cybersecurity from their suppliers.

HOW DO YOU IMPLEMENT VERSION 5?

800-53 Version 5 goes into effect in September 2021. The fundamental steps for implementing it — whether you're migrating from Version 4, or adopting 800-53 for the first time — are straightforward. You map your existing controls to Version 5, identify whatever gaps your security controls might have, develop a remediation plan, and then implement those steps to achieve compliance.

The reality, of course, is more complicated. Version 5 is an exhaustive set of security controls, with wholly new components relating to privacy and supply chain risk. Many businesses are likely to identify significant gaps, or perhaps not even know where to start. Some trying to implement Version 5 today may never have implemented 800-53 in the past.

To help organizations with such challenges, NIST also released 800-53B — a collection of "baseline" controls that an organization can use to start implementation. Those baseline controls are grouped into three sets, depending on whether your security risks are low (say, managing a routine business system for a federal agency), medium, or high (operating systems related to critical infrastructure). 800-53B also includes a set of baseline privacy controls applicable to any business that processes personally identifiable information.

So your 800-53 compliance journey is likely to begin with close collaboration between the compliance and IT security functions. Perform a quick analysis of your organization's overall risk level and threat profile; and then implement the appropriate set of baseline controls from 800-53B. Then conduct a more comprehensive risk assessment, exploring issues such as your use of third parties and exposure to privacy laws. With that information in hand, you can begin tailoring your security controls much more precisely; perhaps adding more controls in some places, or eliminating unnecessary baseline controls in others — while documenting your decisions all along the way.

That still leaves the related question of **why** an organization should implement 800-53 Version 5. The foremost answer: because customers and business partners will expect that high level of effective cybersecurity risk management. Beyond that business imperative, however, 800-53 will also lead to compliance and information security functions working in a more integrated fashion — which will have significant benefits to your compliance program, since privacy and security concerns are seeping into every aspect of business operations. The more you can also embed 800-53 into daily business operations too, the less challenging privacy and security compliance will be.

Every business has its own unique set of IT risks, so every business will need to achieve 800-53 compliance in its own way. That said, we can define certain capabilities that all businesses will need as they move forward with 800-53 compliance.

- **Visibility into the supply chain.** You will need deeper visibility into the security risks of your suppliers, especially your technology and Software-as-a-Service (SaaS) vendors. That means maintaining an inventory of your suppliers, tracking the risk questionnaires you send them, collecting the attestations or other evidence they provide, and so forth.
- **Better data mapping.** You'll need an ability to see what types of data your business creates, processes, and stores; as well as which vendors might touch that data (for vendor risk management purposes) and where the data physically resides (for privacy or e-discovery purposes).
- **Policies and training.** Your single biggest risk will always be employees or third parties mishandling your data. That means developing comprehensive security and privacy policies, supported by training as necessary, and documentation that your policies and training have been rolled out effectively.
- **Risk assessment and gap analysis.** 800-53 has hundreds of controls addressing even more potential security risks. You'll need a sophisticated ability to assess how those risks do or don't manifest in your business, and what remediation steps you should take to close those gaps and achieve compliance.
- **Task management, alerting, and reporting.** Achieving compliance with Version 5 will be a significant undertaking, involving many people and many tasks. The ability to assign remediation tasks will be critical; as will alerting to inform you when tasks aren't getting done, and reporting so you can see your compliance progress at a glance.

The sheer volume of work here also means that **using a tool to manage and automate your compliance tasks** is critical. You simply won't be able to succeed in such a complex, enterprise-wide challenge with manual processes such as spreadsheets to track work and email to chase down required documentation.

HOW DO YOU WORK WITH CISO, BOARD, AND OTHERS ON 800-53?

As you proceed with 800-53 Version 5, another concern will be how to interact with your board of directors and senior management team. Cybersecurity is a top concern for senior leaders, so they should want to know about your progress — but at the same time, compliance with 800-53 will be a major undertaking that involves time, money, and resources. You'll need to consider how to build and maintain support.

First, **frame 800-53 compliance as an investment in risk management and competitive position**, rather than as a compliance exercise. Implementing the standard will help your business to keep attackers at bay, protect confidential information, and win over customers who might be skittish about your company's ability to protect the data they share with you. That's all true regardless of any regulatory compliance obligations you have to implement Version 5.

Second, **stress that compliance will matter more, too.** By 2025, the Department of Defense and other federal agencies will expect all their contractors to meet the standards within Version 5. No compliance means no contracts. Moreover, that demand for Version 5 compliance will extend down through the supply chain — so even if your business isn't a U.S. government contractor, your customers who are contractors will expect you to meet Version 5's standards anyway.

Third, when briefing senior leaders, **summarize the compliance gaps the business has and the remediation work that still lies ahead.** You will want an ability to drill down into specific issues if the board, CISO, or other executives ask, but start with a focus on risks and impacts to the business — not on the details of compliance work.

Fourth, **use dashboards for a comprehensive view of your exposure and remediation progress.** The CISO, privacy officer, and others will want reports on the company's progress. Relying on manual processes to collect and report that status is impractical and won't help you maintain support for the project. A "compliance at a glance" dashboard will — and will save you time and grief as well.

CONCLUSION

SP 800-53 Version 5 will be a transformational security standard for many businesses. To a certain extent we can welcome its new attention to privacy and supply chain risks, and its focus on outcomes rather than control structure.

Still, achieving compliance with Version 5 will be a lot of work. You will need support from senior managers, support from other functions across the enterprise, and a smart technology strategy to automate as much of the compliance burden as possible. You'll need to define compliance with Version 5 as an investment in risk management (which it is), and weave its policies, procedures, and controls throughout your business operations.

The good news is that on the far side of things, your business will emerge ready to do business with the U.S. government and any other corporate customer, because you'll be able to meet the modern threats of cybersecurity. That's a competitive advantage worth achieving, as soon as possible.