Move to NIST Rev. 5 now for a more secure government organization

Tips for smoother transitions

Benefit from a head start

It is true. Documentation for National Institute of Standards and Technology (NIST) 800-53 Revision (Rev.) 5 is incomplete. Published compliance guidelines and timelines for the September 2020-released revision are not yet available. Despite the lack of guidance, do not wait until documentation is 100 percent in place to begin the move from Rev. 4 to Rev. 5. The transition will require planning and detailed work over time that a deadline cannot rush. Government agencies that begin now will be able to implement important controls to enhance security and protect from growing breach issues. In 2021, governments worldwide saw an 1,885 percent increase in ransomware attacks.[1] With security breaches on such a steep rise, each one you stop is worth the effort.

The NIST framework provides standards and guidelines to help ensure federal, state, and local government agencies' systems and devices are secure and resilient. In this article, we highlight potential **issues to avoid** and **lessons learned from successful Rev. 4 to Rev. 5 transitions** that should help CISOs and technology leaders experience a smoother transition. We hope these insights will motivate your agency to **push forward now to create a more secure organization**.

Why modern government is important

Government agencies in the U.S. must modernize in order to keep up with changing user needs, regulations, and health and public safety requirements. Leaders of modern governments rethink business processes and service delivery models to more effectively achieve their mission. This article is one of a series that features how modernizing affects the government workforce and the user experience, improves security and public trust, and accelerates the digital journey. KPMG team members offer insights intended to help guide governments in their modernization efforts to encompass all processes, technologies, policies, and the workforce so each works together to create connected, powered, and trusted organizations.

[1] Source: Fortune, Amiah Taylor, "There's a huge surge in hackers holding data for ransom, and experts want everyone to take these steps," February 17, 2022.

Tips to avoid common Rev. 5 transition challenges

It is critical for tech leaders to identify how new security controls impact their organization since agencies must eventually show how they comply with each control set. The most significant Rev. 5 additions are new **privacy controls** and **security controls** dedicated to **third-party risk** and **supply chain risk management**. While not a new control set, privacy moved from the appendix to the main section and includes new controls related to personally identifiable information processing and transparency.

We recommend visiting the NIST website to learn the primary differences between Rev. 4 and Rev. 5. The documentation explains other differences, which include new controls covering cyber resilience, secure system design, security and privacy governance, and accountability. As the diagram below shows, in addition to **implementing** new controls, **documentation** must reflect Rev. 5 updates. Audits also may involve new **assessment** types.

While working with clients on several successful moves from Rev. 4 to Rev. 5, we documented lessons learned. The following tips can make your transition smoother.

Changes to risk assessments and security programs

Implementation	Documentation	Assessment
New privacy/supply chain requirements and control families must be met to comply.	Legacy documentation must be refreshed to match the reorganized controls and control families.	Audits may involve new assessment evidence types.

Avoid capability and tool challenges

- No capability, tool, or platform an agency uses is compliant with Rev. 5 **until all capabilities, tools, and platforms comply**.

- **Rev. 5 merges security and privacy** and embeds both throughout the process. With this change, CISOs and privacy officers must combine capabilities and align roles and responsibilities.

- **Teams focusing on Rev. 5 implementation across many security domains** will find establishing a **central platform** for collaboration, communication, and document tracking will improve their capability to deliver transition updates and enable a smoother transition.

- **Organizations that use cloud environments cannot comply with Rev. 5 yet.** While the controls were available in 2020, NIST published the instructions on how to use the controls in 2022, so cloud service providers are still working toward compliance.

- **Do not fear an audit.** Some government tech leaders are more afraid of a new external audit notice and a large number of findings and recommendations than actual vulnerabilities. Rev. 5 pushes controls into place that protect against real villains.

- **Villains should serve as motivation for agencies to find vulnerabilities.** There are no 100 percent secure systems, so those with single digit vulnerability rates are rare. Finding more vulnerabilities will move your organization further toward maturity. When you find weaknesses, reassess and learn from there. Your organization will be more secure.

- **Monitor security control compliance.** Include Rev. 5 controls in A-123 control assessments to better monitor internal control effectiveness.

Without roadblocks, you can begin

- Organizations cannot go wrong by moving to Rev. 5. **It is okay to make mistakes if you move forward.** Learn along the way until the guidelines are available.

- Tech leaders must **analyze each new control** to determine if it is relevant to the organization. This step will help prioritize and make the transition less overwhelming.

- Identify controls that have the **most valuable impact to the organization for the investment and start there**. Then move to other areas to progress until NIST publishes guidelines.

- **Updating procedures to meet Rev. 5 expectations is more difficult** than identifying and aligning differences from Rev. 4 because it is subjective. Using a comparison method, as described in the section below, can be an effective procedure update method for many agencies.

- **Collaborate with top stakeholders** throughout the process for a smoother, more sustainable implementation.

- **Train team members** on new requirements and updated procedures so they understand how it affects their work to improve new controls adoption.

Method helps tech leaders rewrite policies and procedures

Procedure updates challenge agencies most. Teams must rewrite all policies and procedures based on the Rev. 5 controls. It is an enormous task. This means leaders need to understand how to change procedures across security domains to meet the new modifications.

A **comparison method can be successful** with agencies. CISOs can compare and analyze their organization's baseline control set against NIST 800-53 Rev. 4. They use what they learn to implement Rev. 5 privacy and supply chain risk management control domains. The analysis can include deleting and/or modifying existing controls and adding new Rev. 5 controls across the organization. The comparison will also help leaders identify gaps and design the right policies, procedures, and processes for a smoother, more sustainable implementation.

Core to success is **aligning security controls to procedures**. The team responsible for aligning current procedures to new security control procedures needs institutional knowledge of the organization and to be aware of the workstream to collaborate and understand what procedures need updating. They must also make sure new procedures fit into updated controls.

IT infrastructure must also match Rev. 5 components and controls. Office of Management and Budget Circular A-130 includes information system management guidance.[2] The plan can look great on paper, but agencies must also prove they updated the IT infrastructure. This guidance can help.

Take the right first steps

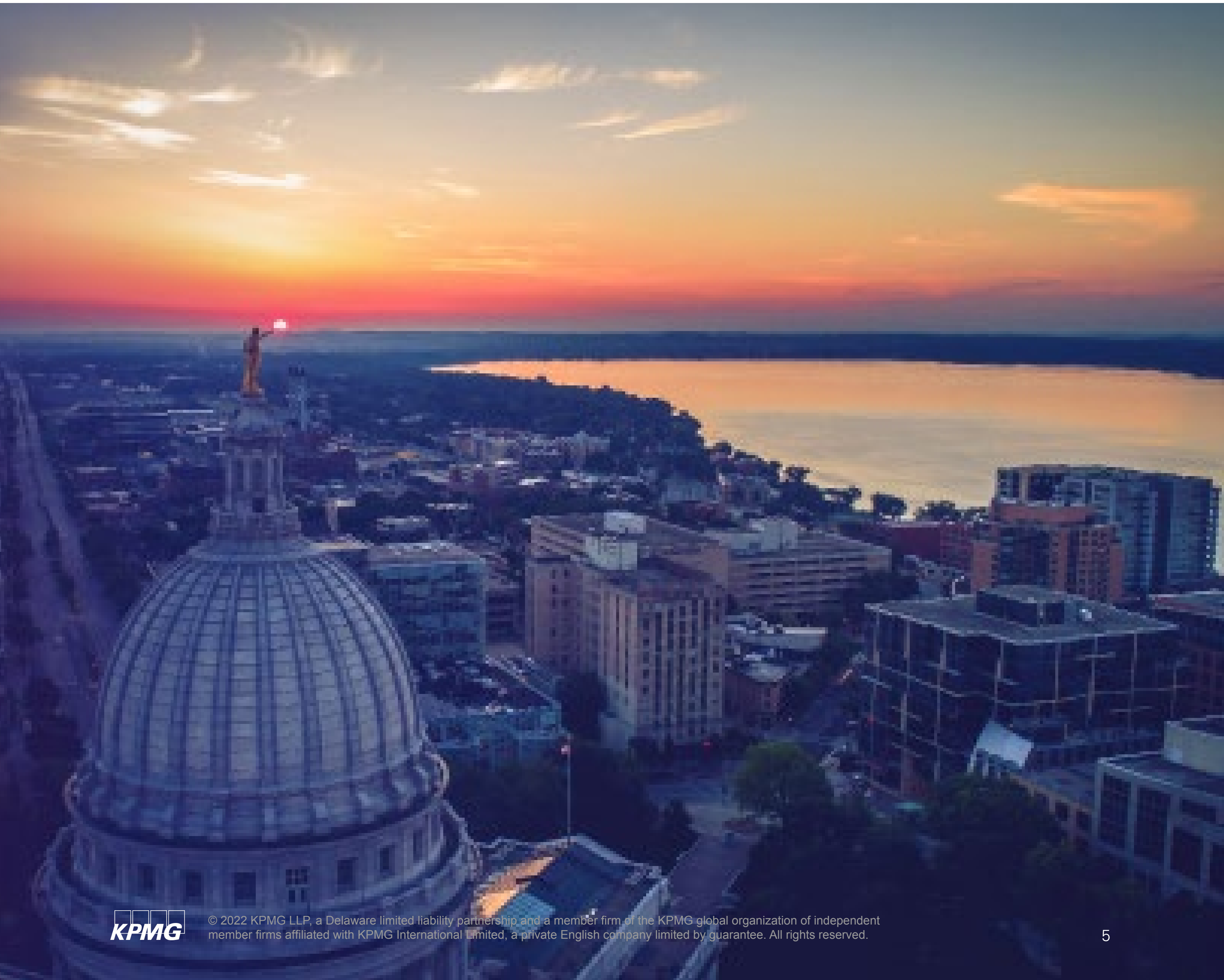
Many tech leaders are waiting for guidelines, someone to tell them what to do first. Our teams have already helped multiple government organizations successfully transition from Rev. 4 to Rev. 5. We combine the team's knowledge and experience with templates and solutions to help agencies comply with minimal distraction from daily operations. Our team also helps establish a project management office for tracking Rev. 5 milestones. Do not stop in a holding pattern. Move your program forward and learn along the way. A more secure, resilient organization is worth the effort.

[2] Source: Office of Management and Budget, "Managing Information as a Strategic Resource," July 2016.

About KPMG

KPMG has worked with federal, state, and local governments for more than a century, so we know how agencies work. Our team understands the unique issues, pressures, and challenges you encounter in the journey to modernize. We draw on our government operations knowledge to offer methodologies tailored to help you overcome these challenges and work with you from beginning to end to deliver the results that matter.

The KPMG team starts with the business issue before we determine the solution because we understand the ultimate mission. When the way people work changes, our team brings the leading training practices to make sure your employees have the right knowledge and skills. We also help your people get value out of technology while also assisting with cloud, advanced analytics, intelligent automation, and cybersecurity. Our passion is to create value, inspire trust, and help government clients deliver better experiences to workers, citizens, and communities.



Contact Us

Tony Hubbard
Principal, Government Cyber Security Leader
KPMG LLP
202-486-4945
thubbard@kpmg.com

Joseph Klimavicz
Managing Director, Federal CIO Advisory Leader
KPMG LLP
703-795-8999
jklimavicz@kpmg.com

Kathy Cruz
Director, Government Cyber Security Practice
KPMG LLP
916-792-3976
kathycruz@kpmg.com

read.kpmg.us/modgov

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.