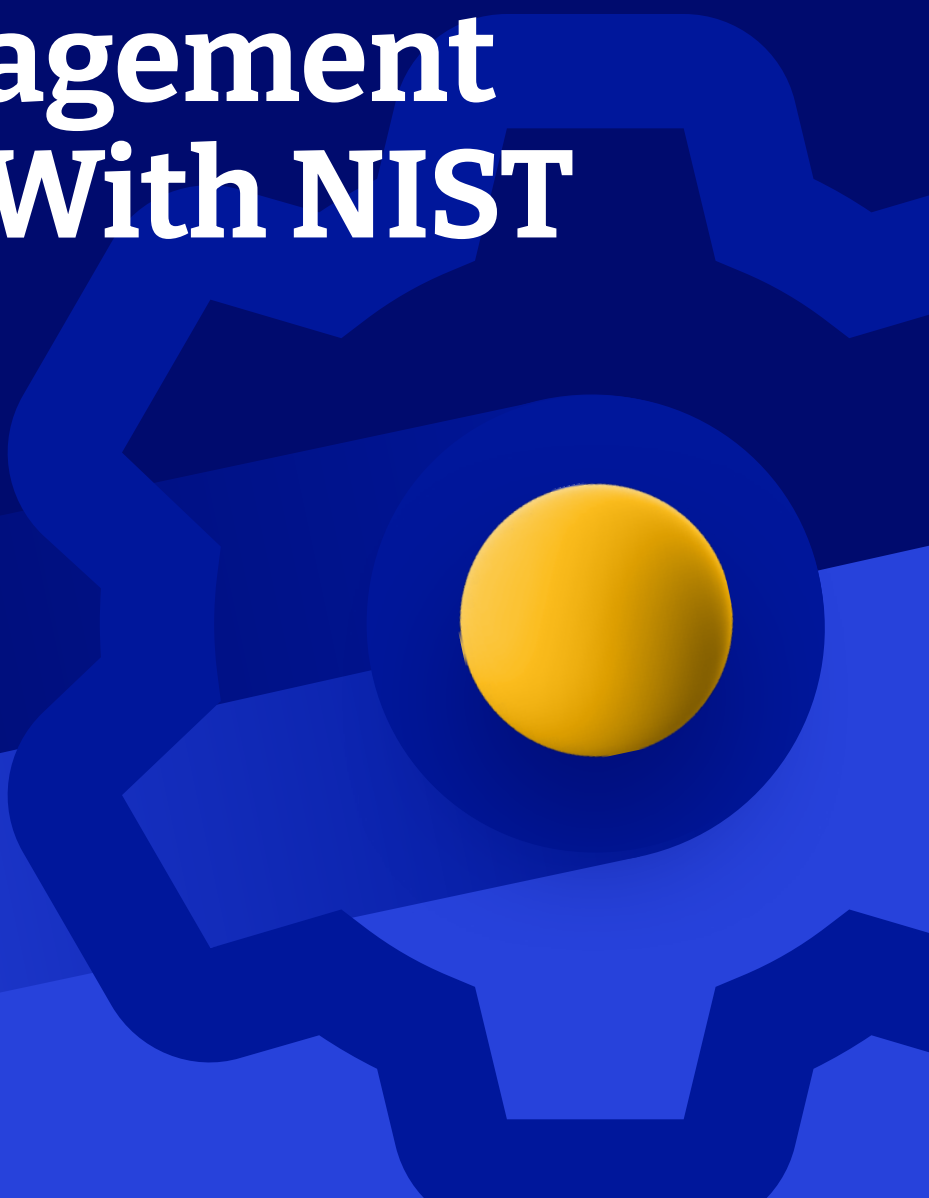
ZenGRC

eBOOK

HOW TO

Upgrade Your Cyber Risk Management Program With NIST



zengrc.com

For many organizations in the public sector, NIST special publications 800-53 and 800-171 serve as the golden standard to building a cybersecurity program that protects your data, services delivery and market reputation.

NIST is often the next step after an initial SOC 2 report for maturing companies looking for something more granular and stringent.

Plus, as many other compliance standards are built upon NIST cybersecurity protocols—such as ISO 27001 and CIS CSC—NIST is the natural choice to take a cybersecurity program to the next level.

Thus, NIST provides a critical common language and foundational security standard that, when implemented, provides a more mature, robust cybersecurity program.

IN THIS GUIDE, we'll outline NIST objectives and the differences between NIST 800-171 and 800-53 along with a checklist to help you get your organization started with NIST compliance.

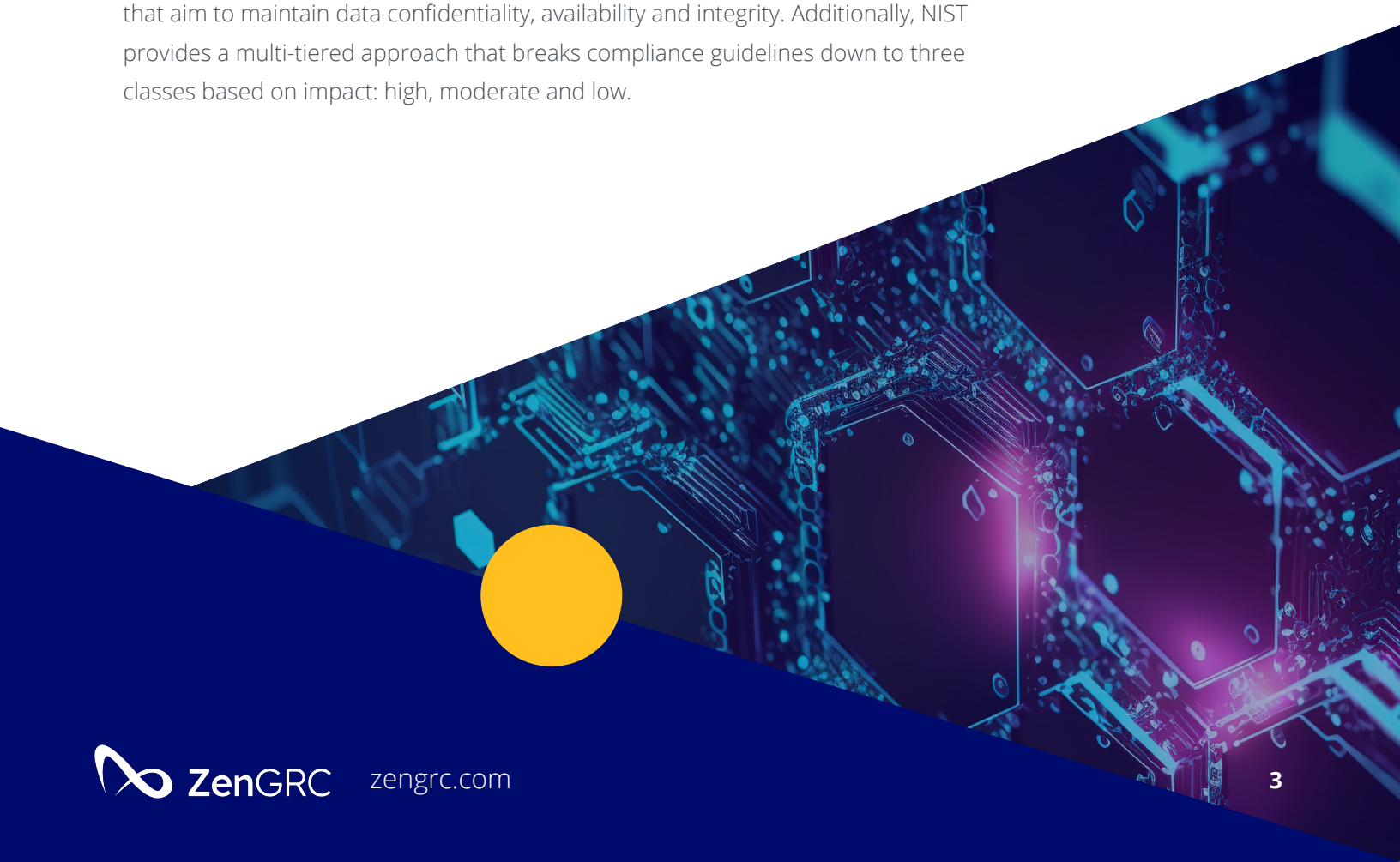
NIST Objectives

In general, the objective of the National Institute of Standards and Technology (NIST) is to promote industrial competitiveness and innovation in the United States by creating standards for the measurement of science and technology and improve economic security.

NIST 800-53 is the de facto standard for private businesses that do business with the U.S. federal government. Note that in moving from rev4 to rev5, NIST dropped the "US Government" focus for NIST SP 800-53 and now has it generalized enough for private industry to use. NIST 800-171 specifically covers the recommended security requirements for protecting the confidentiality of controlled unclassified information (CUI) when it lives in nonfederal information systems and organizations.

NIST 800-53 has 20 control families and NIST 800-171 has 14 control families that represent the core categories of a robust cybersecurity program and support the implementation of secure and federal information systems.

These controls incorporate technical, operational and managerial best practices that aim to maintain data confidentiality, availability and integrity. Additionally, NIST provides a multi-tiered approach that breaks compliance guidelines down to three classes based on impact: high, moderate and low.



Examples of NIST controls

ACCESS CONTROLS

NIST can help you implement a complex logging system, control which team members have access to sensitive assets and how team members safely access systems remotely.

CONTINGENCY PLANNING

The NIST contingency planning control family provides guidance aimed at helping organizations plan for business continuity in the event of a cybersecurity event. Individual requirements include employee training, plan testing, system backups and system reconstitution.

RISK ASSESSMENT

The risk assessment control family outlines how an organization should define its assessment and vulnerability scanning policies. This includes both the methods for conducting risk evaluations, frequency of testing and team awareness training around risk assessment.

NIST 800-171 vs. 800-53: Which Should You Choose?

NIST 800-171 and 800-53 are two of the most frequently used special publications companies use to further their cybersecurity programs. So which should you use to guide your cybersecurity program? The answer is: it depends.

Both seek to provide a comprehensive and flexible catalog of current and future protection controls based on changing technology and threats. Both seek to develop a foundation for assessing techniques and processes for determining control effectiveness.

Both aim to improve communication across organizations via a common lexicon for discussion of risk management concepts.

However, they also have some distinct differences.

NIST 800-53

NIST 800-53 is a security compliance standard from the U.S. Department of Commerce in response to the quickly evolving technological capabilities of national adversaries.

NIST 800-53 is mandatory for all U.S. federal information systems except those related to national security. The guidelines in 800-53 are also helpful for any organization utilizing an information system that houses or processes regulated or sensitive data.

NIST 800-171

On the other hand, NIST 800-171 covers recommended security requirements for safeguarding the privacy of controlled unclassified information (CUI) when the data lives in nonfederal information systems and organizations.

NIST 800-171 applies to any organization that transmits, stores, or processes CUI for the Department of Defense (DoD), NASA, the General Services Administration (GSA), and other federal or state agencies as dictated in 800-171.

Checklist: Get Prepared for NIST

Once you've determined that NIST is the right next step for you, there are some general best practices you can use to help you prepare for attestation.

DETERMINE WHICH NIST FRAMEWORK (800-53 OR 800-171) YOU WANT TO IMPLEMENT

- ◯ Establish your objective and scope based on the appropriate NIST controls

IDENTIFY AND CLASSIFY YOUR SENSITIVE DATA

- ◯ This includes mapping the data to all systems that house, transmit, or process that data

ASSESS YOUR CURRENT LEVEL OF CYBERSECURITY WITH A NIST 800-171 OR 800-53 ASSESSMENT

- ◯ This process will help you to identify your gaps and where you're doing well so you can prioritize any areas that are lacking

DESIGN A COMPLIANCE PROCESS TO ASSESS YOUR ORGANIZATION

- ◯ While many begin with spreadsheets, these are unreliable and don't scale well over time
- ◯ Ensure the chain of command for risk mitigation and escalation. This should include a method for following up and ensuring accountability
- ◯ Allocate the necessary resources to carry out your plan

CREATE YOUR PLAN OF ACTIONS & MILESTONES (POA&M)

- ◯ This will include updating your existing security policies or introduce new ones to align with the appropriate controls

COMMUNICATE SECURITY POLICIES TO YOUR EMPLOYEES AND ENSURE THEY UNDERSTAND THEM

- ◯ Establish secure communication channels for collecting sensitive evidence artifacts
- ◯ Awareness and training should be a key component of your program

MAKE COMPLIANCE AN ONGOING PROCESS

- ◯ In other words, find a reputable software solution like ZenGRC that can help you keep tabs on your compliance and risk stance over time

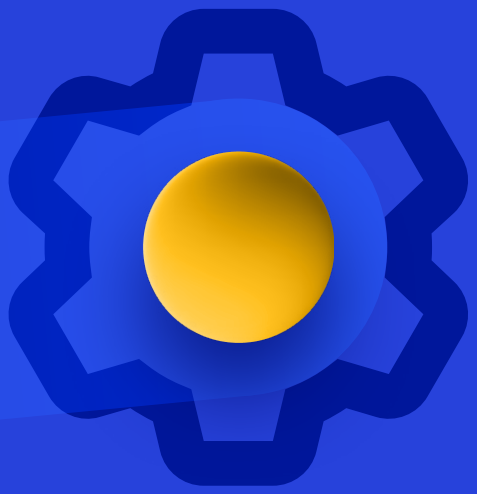
How ZenGRC Can Help You Get Started with NIST

Managing cybersecurity risk and compliance is not a one-time project. It's an ongoing effort that must be closely adhered to. Otherwise, it loses its effectiveness as regulations change and cybercriminals get smarter.

ZenGRC can help you put this checklist into action by simplifying day-to-day compliance management and making it easier and more efficient to manage multiple compliance programs at once. It eliminates tedious manual processes and reduces the number of human resources required to deliver positive audit results, setting you up for a successful NIST implementation.

Ultimately, this means streamlined compliance, fewer business disruptions, better visibility into compliance and risk status and a future-proof path to compliance and security for your business.

Ready to learn more about ZenGRC?



SCHEDULE A DEMO

READ MORE ON NIST

ABOUT ZENGRC

Founded in 2009, ZenGRC is a leading governance, risk, and compliance (GRC) SaaS solution provider, offering two robust products: ZenGRC and ZenGRC Pro. Recognized for its in-house GRC expertise, ZenGRC delivers Simply Powerful GRC solutions that guide organizations through compliance with ease and efficiency.

ZenGRC stands out by offering a single price for comprehensive access to all modules and frameworks, ensuring users benefit from a seamless and cost-effective experience. Dedicated to simplifying GRC processes, ZenGRC continues to innovate and support organizations in achieving compliance and managing risk effectively.

Simply Powerful GRC

zengrc.com