ZenGRC

Preparing for a NIST Audit

A Step-by-Step Guide

www.zengrc.com

The National Institute of Standards and Technology developed the NIST Cybersecurity Framework (NIST CSF) specifically to aid in securing our nation's critical infrastructure—but it is useful for almost any organization. A thorough compendium of information security rules and guidelines, NIST can be an invaluable resource for improving your enterprise's security posture.

Checking off the NIST list assures your enterprise, customers, and clients that your systems, networks, and data—and their data, as well—are safe from intrusion. Implementing NIST CSF will also save you time, effort, and expense down the road, bringing you into compliance with other security frameworks, including PCI DSS and SOX.

NIST also developed NIST 800-53, a set of controls to help with NIST CSF compliance, which is voluntary, as well as compliance with other frameworks. NIST 800-53, considered the cybersecurity bible among federal agencies, specifically governs compliance with the Federal Information Processing Standard Publication 200 (FIPS 200), mandatory for government-affiliated entities.

NIST 800-53 contains hundreds of controls. Navigating compliance can feel overwhelming. Fortunately, the framework is highly prescriptive, in many cases spelling out not only the what of compliance, but also the *how*.

Whether you're working with the government and require FISMA compliance, or yours is an enterprise using NIST guidance for aligning to other security frameworks, an organized approach will help you reach your compliance goals.

Follow this comprehensive checklist compiled by our experts to make NIST compliance as easy as 1-2-3.

TAKE ME TO THE CHECKLIST

Revision 5's Focus: Privacy

Previous versions of NIST 800-53 focused on preventing data breaches and thwarting system security attacks through an emphasis on confidentiality, availability, and integrity. Revision 5 adds privacy to the mix.

In response to the proliferation of data privacy laws across the globe, Revision 5 addresses the creation, collection, use, processing, storage, maintenance, and dissemination of personally-identifying data as well as the privacy risks associated with this type of data.

NIST 800-53 Revision 5 has 20 control "families":

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

1. Access control

This family addresses access controls for your organization's IT environment: routers, firewalls, computers, servers, and all devices on the network. It considers how these are configured as well as the quality of your security policies, role-based access controls, mandatory access controls versus discretionary ones, and privileged access controls.

- Who has access to your systems, networks, and devices? How do you grant access? How do you restrict it? Do you allow any users to override access controls? Which ones? What is the procedure?
- How do you grant access to third-party vendors?
- What attributes do you use that affect access?
- Have you documented your information flow control policies?
- How do you separate and isolate FedRAMP-certified devices and systems?
- Do you have a comprehensive list of your domains and cross-domains? You will need an inventory that includes individuals with access to these domains, their roles and responsibilities, and their associated controls.
- Can you provide role-based schemas for your privileged access accounts? Do you use dynamic account management or shared or group credentials for these accounts?
- Are you embedding access controls into your metadata? You will need to define and identify this data.
- What are your domain authentication processes and policies? How do you spot violations?
- Do you tag access data for quick identification? Many companies have done so since
- the enactment of the European Union's General Data Protection Regulation (GDPR) so that if access control data is changed, those changes can be identified quickly.
- When account data is changed, who gets notified? Does your system track the nature of the changes, what data has been captured, and session login and termination times?
- Who has remote access to your systems, and how is access granted? Do external networks gain access via dial-up, broadband, or a virtual private network? Do users log in automatically? Which credentials do they need to gain access remotely? Which prompts and commands require them to validate their identity?

- For wireless access, what is the authorization process? Is the data encrypted? What are the devices' encryption settings, and what security controls do they contain? Devices include smartphones, mobile phones, laptops, e-readers, tablets, and any external systems.
- Who is allowed to set up configurations? Who has access to information using
- automated scripts or application programming interface (API), and who can make
- changes in these configurations?

2. Awareness and training

These controls examine your organization's internal security-and-privacy awareness training.

- What type of security awareness training do you provide? Do you review and update your training policy annually? How do you disseminate the security awareness policy to your employees?
- What does your training include? Auditors expect training on malicious phishing, malware, email breaches, social engineering, and other cybercrime tactics.
- How do employees access the training?
- How do you notify employees about security vulnerabilities, malware, suspicious communications, and other security concerns? In the case of a cyberattack, how, when, and where do you send notifications? Are you continually monitoring your system for these threats and sending alerts in real time? Do you instruct employees on what to do? Do you follow up?

3. Audit and accountability

For this control category, you will need the details of your organization's audits and audit processing records.

QUESTIONS INCLUDE:

- How do you process your audits? How do you monitor them? How do you set up the content for your audits? Do you include assessments and artifacts?
- How is audit information captured and collected?
- How does audit information get modified? What's the chain of custody?
- How do you store your audit documents, and where?
- Are your audit documents time-stamped?
- How do you protect audit information? What encryption tools do you use?
- Who is authorized to access audit information? How do you validate their identity—with passwords, multi-factor authentication, biometrics, or some other method?
- What is your retention policy for audit information? How do you retrieve it?
- How do you track and document audit trails so that you know who has accessed or made changes to audit documentation? Audit trails should include the time and details of the changes.

4. Assessment, authorization, and monitoring

QUESTIONS INCLUDE:

- Who conducts your organization's privacy and security assessments? What are their roles? Do you perform these in-house or use independent third parties?

- What are your privacy policies and procedures for setting up privacy and security assessments and monitoring?
- When do you conduct assessments? How often? What type of assessment does your enterprise perform—security only, or do you assess privacy protection as well.
- What types of specialized assessments do you perform—open testing, validation testing, and/or vulnerability scans?
- Do you monitor your systems, applications, and network?
- What are your privacy controls? Do you monitor them?
- If you are FedRAMP-certified or pursuing that certification, do you scrutinize your system's interconnections, interfaces with internal or external systems, and boundary-protected devices? Are these devices and systems securely isolated from the rest of your network?
- Do you have controls, such as blacklisting, for malicious domains?
- Do you assess and monitor secondary or tertiary connections or interfaces with outside systems?
- Is your monitoring continuous? If not, how often does it occur? Be prepared to present your analysis and trend reports.
- Do you conduct red-teaming? What does it consist of, and how often does it occur?

5. Configuration management

The auditor will want to see your configuration management policy and procedures.

- How often do you review these documents? Do they discuss privacy? What are your baseline configurations? Are they delineated for every server or device on your network? Do your configurations include security or hardening of those devices?
- Do you use automation for configuration management? What kind?
- Do you retain previous configurations or settings? Do you have the ability to revert to them in case of server issues? What is your rollback process? How do you uninstall problem applications and programs, and conduct updates?

- Do you have configuration and testing settings for your development and testing environments? Are those environments separate?
- Do you have a Configuration Control Board to ensure that
- configuration changes get approved in an orderly manner?
- What is the process for change validation?
- Do you have a process to ensure that your software or hardware is tested and validated before it moves into production? What is that process?
- What are your cryptography settings? Are configurations documented?
- What is the review process for your security policy? Are there any restrictions on policy changes or access? Have your security policy on hand for the auditor's review.
- Do you have an inventory of all your system components? Be prepared to show this.
- How often do you update it?
- How often are installations and deactivations added to the systems inventory? Is this
- automated? Is there a centralized repository?
- Do you have data maps?
- Is there personally identifying information (PII) within your systems? Do you have a legal and valid business purpose and use?
- Do you have a configuration management plan? Be prepared to show it to auditors. It should include:

  - The software development lifecycle Items under configuration management
  - Policies and procedures for making changes and requesting updates
  - Automated update processes

- Do you allow users of enterprise devices to install software? If so, what are the policies and procedures for doing so? What are the limits?
- What are your controls or processes for installing software on new or existing servers?

6. Contingency planning

Have on hand your organization's contingency plan for keeping the business running in case of a system outage, cyber event, or catastrophe.

- If an outage occurred, how quickly could your systems, including critical systems, be up and running again?
- Do you have an alternative way to conduct business in case your systems shut down?
- Do you have an alternative system for data capture, processing, and storage? Do you
- have systems in multiple locations?
- Have you identified your critical assets—those to restore first?
- Have you identified your automated continuous transactions, such as human resources and financial systems or critical system integrations? Do you have a plan to continue business in case of a shutdown?
- How long can your business operate without data? What is your recovery time?
- What is your Recovery Point Objective? This should include the files and age of files to recover and upload to your alternative site so business can resume.
- How much data can your enterprise afford to lose?
- How long can you weather an outage before losing business?
- What is your Recovery Time Objective (the time you need to recover your data)?
- How often do you back up your systems?
- Do changes to your primary site automatically sync with your colocation site?
- Do you have a record of changes made to your system between 90 days and 6 months ago? Were those changes also made to your colocation site?
- Be prepared to present documents showing your:

- System components
- Network topology
- System architecture
- Configuration management tools in use
- The currency on which these systems run
- Rollback policy
- Backup retention policy
- Modifications to your hardware
- Reports of configuration testing on your primary and colocation sites
- Automation changes

- Does your organization use an API? If so, have you set up an Electronic Data Interchange, as well?
- Have you tested your contingency plans? If not, how do you know they work?
- Do you have a formal disaster recovery plan? Is it reviewed annually or when new systems are added?
- What disaster recovery training do you provide? Who receives it, and how often?
- Do your disaster recovery policies and procedures address your primary and colocation sites both individually and separately?
- What agreements do you maintain with your telecommunications providers and other third-party vendors in case of disaster?
- Do you have a "single point of failure"—only one system and server, with no other systems to capture information in the event of a disaster? If so, your system's design is flawed and should be corrected.
- What are your policies regarding system redundancy and data transfer? How is information transferred to your backup site? Is it done automatically? Where is the information stored, and for how long? Is it encrypted?
- Is your colocation site on "hot standby," meaning that you can switch your IT operations over and resume running within minutes of losing your primary system?

7. Identification and authentication

Be prepared to show your policies and procedures for identifying and validating users of your systems, networks, and devices.

- Do you use multifactor authentication for users as well as for privileged access accounts?
- How do users sign on to software? Do they use single or dual authentication? Are they authenticated each time they sign in, or only once?
- What are your logical access controls and physical access controls?
- How do you authenticate devices?
- Do you use dynamic or static IP addresses?

- What level of complexity do you require for passwords?
- How often do you require password changes?
- Do you use biometric authentication?
- What public key structure do you use for encrypting data?

8. Individual participation

What does your privacy policy say about collecting, storing, or processing PII? Have the policy on hand for the auditor.

- Which categories of PII data do you capture?
- Do you obtain consent before collecting, processing, storing, or transmitting data?
- Do you provide a “just in time” notice—one that condenses your more-lengthy privacy policy into short, easy-to-read segments presented to visitors of your website?
- If someone wants to correct, change, or remove their data from your database, what are the procedures for redress? Is there an appeals process?
- Do you issue notices of correction or amendment to owners of PII?
- Do you allow PII owners to see their data and approve changes, amendments, or corrections?

9. Incident response

If your systems were breached or attacked and your data were exposed, what would you do?

- Do you have an incident response policy? Have it ready to present to the auditor. Has senior management or an executive management team approved your organization's incident response policy?
- Does your enterprise conduct incident response training? Do you use red teams?
- Simulated events with root cause analysis?
- Have you tested the latest version of your incident response plan?
- Do you strive for continual improvement of your incident response metrics, such as incident response time and recovery time? Do you record lessons learned?
- Do you use an automated incident response tool? Does it include automatic disabling of all or, at a minimum, affected IT systems?
- How often do you review and test your incident response plan? Do you do so at least once a year?
- If you have more than one critical system, how do you coordinate and communicate security incidents across systems?
- Do you have a policy or mechanism for alerting third-party vendors to a breach?
- Do you have incident monitoring in place for your systems and applications? Is analysis included? When are alerts sent?
- Do you use a security information and event management tool for tracking, alerts, and log generation?
- In case of a major security breach, who at the local, state, or federal level would you need to contact? Are you in communication with them? When and how would you send these alerts?
- Do you use a vendor for incident response?
- Do you check your IT scan reports for system vulnerabilities? Who performs this task, and how frequently? What is the procedure for fixing any flaws? Who is responsible?
- Who reviews and updates your incident response plan, and how often? Who has a copy of the plan? Do employees have it? Have they been trained on how to follow its directives?
- Who has the ultimate responsibility for incident response at your organization?

10. Maintenance

- How often are diagnostics and repairs performed on your systems? Does systems maintenance occur in a controlled environment? Who has access to perform maintenance?
- How do they gain access if the system contains confidential data?
- How often do you perform maintenance on your systems?
- Which maintenance tools does your organization use? Do you have specific media for this task, such as a designated drive?
- What are your contingencies for drives or networks that may be affected or interrupted during systems maintenance?
- Who gets notified of maintenance activities? When are these notifications sent, and how?
- Who is responsible for approving maintenance-related downtime? What is the approval process?

11. Media protection

- Who has access to your organization's IT media, including storage media? This includes your servers, databases, backup tapes, memory cards, rotating fixed disks, hard drives, and solid-state drives.
- How is this media handled and stored? Is it encrypted?
- Who are the media custodians?
- How is this media maintained?
- What are your policies and procedures for decommissioning and destroying IT media?
- Is it backed up before destruction? Does it get erased?
- What happens to the backup data when media is destroyed or decommissioned? Does it get classified or tagged?
- Who handles media destruction or decommissioning? Is this performed in-house or by a third-party entity?
- When does media get destroyed or decommissioned? What are your policies and procedures? Be prepared to show this documentation to the auditor.

- If your organization does not destroy decommissioned devices, such as laptops and other mobile computing devices, why not? What happens to these devices instead?
- Who signs off on media destruction? Are at least two people responsible for authorization?
- How is data removed from media? Is it done in-house, at a vendor's location, or remotely?
- What measures do you take to protect PII? Do you anonymize or pseudonymize it for data minimization? Is this data backed up before destruction? Where do you keep copies of this data, and how? Is it encrypted? How long do you keep it? Are you familiar with applicable laws governing the handling of PII data?
- How do you document your handling of organizational IT media and storage? Be prepared to show records to the auditor.

12. Privacy authorization

This control family examines your organization's authority and legal justification for collecting private information.

- What are your privacy policies and procedures? Be prepared to provide them to the auditor.
- What PII do your systems capture?
- What notices do you provide to owners before collecting their PII?
- Why are you capturing PII? You must document your legal business justifications.
- Are you tagging and classifying the PII you collect?
- How do you collect and store PII? Do you use an automated system? What is the process?
- How does your system identify the captured information and its owner?
- Do you share PII with any third parties? Do you monitor the handling of this data?

13. Physical and environmental protection

This category examines your organization's means and methods of ensuring that your buildings, rooms, and environment are secure.

- What does your security policy say about security and physical access to your grounds, buildings, and internal environment?
- Do you maintain an up-to-date employee list?
- What credentials does your organization provide to visitors, employees, and contractors? How often is that list of credentials updated?
- Do you grant access according to roles and responsibilities? What type of identification do you require from visitors? Do you require at least one or two forms of ID?
- Do you restrict access to your buildings and environment?
- How do you monitor visitor access? Do you keep logs and use closed-circuit television to track visitor movements and activities?
- Do you issue security badges to employees and visitors? Can they use the badges to move between floors or buildings?
- Do your buildings have security keys? How often do you change them?
- Does your building have ingress or egress controls? Access devices? Other barriers?
- Do you guard or monitor your IT hardware locations? Is your hardware locked in racks, casing, or cages?
- Are there locks on your office doors? Are employee laptops locked down, for instance at docking stations? Are other devices, including transmission hardware such as cables and routers, physically secure?
- How does your organization monitor your physical premises and access to it? Do you use sensors, video surveillance, or other methods? How are intrusion alerts set up, and who gets notified and when? What are response procedures?
- What are your retention policies regarding surveillance recordings and data? For how long do you keep this information?

- What are your policies and procedures for emergency shutdowns? Do you have uninterruptible power supply systems in case of fire or loss of power? Do you have an alternative power supply in case of an extended outage?
- If a fire were to occur and shut down power, do your buildings have emergency lighting?
- Do they have fire detection and suppression systems? Are those systems activated automatically, or is someone notified to activate them manually? Who gets the notification and what are the procedures?
- How often do fire inspections occur in your buildings?
- What are the temperature and humidity controls in your data center or server environment? Are these controlled automatically? How are they monitored?
- Do you have water and fire detection systems in your server and network rooms? How do you safeguard these from damage?
- What are your procedures for equipment delivery and removal? Who authorizes these
- deliveries, and how are those authorizations reviewed?
- How do you protect your colocation site? Do you know where all your assets are located and how they are protected? How do you monitor and track them?
- Have your asset inventory report on hand for the auditor to review.

14. Planning

This category considers how your enterprise plans and coordinates IT security activities with other organizations.

- Do you have restrictions on social media and networking, and on access to public websites?
- Do you share your operational plans and architecture plans? With whom?
- Do you have a privacy plan? What are your privacy plans and policies, especially concerning coordination and sharing with outside organizations?
- Do you have a security plan? Does it take a “defense-in-depth,” multi-layered approach to defense and security?
- Does your security plan include baseline configuration settings? Does it include customized systems and configuration settings? These should be documented, as well.

15. Program management

- Do you have a program management organization or office? Do you have a project plan listing IT programs that are due for installation or upgrade?
- How is it validated? Do you update it annually?
- Does your project plan include hardware requirements, impacted systems, and dependencies associated with installing or upgrading software or hardware? Who has access to these systems, and how are they notified of changes and their effects?
- Have you planned for information security program roles, resources, actions, and milestones?
- Does your plan include updates to your system inventory?
- How do you monitor and measure projects or programs? How do you track program removal and replacement?
- Does your project plan list include technology to be installed and instructions for aligning it with your current system and data privacy requirements?
- Along with your project plan, you should be prepared to provide your auditor with the following:

  - Critical infrastructure plan
  - Risk management strategy
  - Change management plan

- For each program listed, does your project plan address:

  - Potential threats posed by implementation? Associated roles and responsibilities? Testing and monitoring policies and procedures?
  - Stakeholders involved, including your program team, third-party vendors, the IT security department, a red team, and help desk support?
  - Are all stakeholders aware of the program?

- Are new programs added to your threat awareness process? Has the information associated with each new program been classified? This is especially important for PII.
- Does each program have a privacy plan (if relevant)? This should include assurance disclosures.
- Do you have a data quality management process for new programs?
- Do new programs include automated systems to collect personal information? Do they tag, minimize, and archive personal data?
- Do you have a data integrity board? Is there a process for addressing complaints regarding the collection, processing, storage, and transmission of personal data?
- Who is ultimately responsible for the data captured by these programs and systems?
- Ideally, a senior data privacy official or officer should be in charge of ensuring data privacy, managing your inventory, reviewing data classification categories, and tagging, managing, and reporting risks.

16. Personnel

What are your policies and procedures for vetting personnel to safeguard the security of your organization?

- Do you have clear definitions for all roles and responsibilities, including security roles? What are your personnel screening practices at the time of hiring and termination?
- What are your onboarding and termination processes?
- Do you require personnel who handle sensitive data or intellectual property to sign non-disclosure agreements?
- If employees are transferred or their roles and responsibilities change, how do you ensure that their access to your systems is reviewed and updated so that they have access only to the areas necessary for their job?
- How do you know when someone has violated the terms of their employment agreement, especially regarding privacy and security? What are your organization's punitive measures? Do you remove access, terminate the employee, or something else?

17. Risk assessment and risk management

What are your risk management and risk assessment policies and procedures? Have documentation on hand for the auditor.

- Have you categorized or classified your information by security level? NIST has established standards for categorizing information and systems according to their risk level.
- Are risk assessment reports provided? To whom, and how often?
- Do you use vulnerability scans to identify risks to your applications, servers, and network? How often do you perform scans? What type of scoring system do you use?
- Do you use a component vulnerability scoring system? Is it part of your risk management risk register process?
- How deeply and broadly do you scan your servers for vulnerabilities?
- Who reviews your scanning reports?
- How is the information generated in these reports used? Does anyone analyze trends?
- How many scanners do you have?
- What happens to your historical vulnerability data?
- How do you deal with Severity 1, 2, or 3 vulnerabilities?
- What is your process for assessing the effects of your vulnerability scans on privacy?
- The EU's GDPR requires data protection impact assessments for all critical analyses of your vulnerabilities.

18. Systems and services acquisition

For NIST compliance, you will need to show an acquisitions policy and procedures document for systems and services including resource allocation, capital planning, budgeting, and privacy and security protection for new systems.

THE DOCUMENT SHOULD ANSWER:

- How is development testing and integration carried out for new systems or services? How often are updates and patches scheduled? Do you use live data? What is your acquisition process? Does it include security reviews, and how do you conduct them?
- What are your requirements?
- What are your procedures and requirements for server provision? What are the criteria for acceptance?
- What are your risk review procedures for new systems and services? What security controls must be implemented? Make sure to document them, as well as:
    - APIs
    - Hardware schematics
    - Developer involvement required to activate the new system
    - Data migration requirements
- Are you selecting off-the-shelf systems, or customizing? Are the new systems controlling, storing, or processing government data? Do you have configuration management for the new systems? Key management? What kind? Do your new systems require additional configuration or special installation?
- Have you notified your engineering department and data center? Have you given all the necessary personnel access for installation?
- If the new systems are external, have you made sure that they are secure before using them?
- Have you checked the external vendor's System and Organization Controls for Service Organizations (SOC) report to ensure that, as the host, they have the proper protections in place to secure your data? If not, once you access the external server from your network, you're exposed to unacceptable risks.

- Have you made changes to your configurations because of the new systems or services?
- If so, you will need to provide documentation of those changes.
- If you have new hardware or firmware, have you verified the security of user software
- connections?
- Do you use data mapping to transfer data into the new system?
- Have you performed penetration testing on the new system?
- Have you included the new system in your incident and event monitoring? Is it in your
- incident plan and any security tracking tools you use?

19. Systems and communication

Be prepared to provide your systems and communications policies and procedures documents.

- These documents should address:

  - The included interfaces and applications, how they're partitioned, and the related security functions
  - Hardware separation and software or hardware segmentation
  - The access and flow of information through your systems
  - Shared system resources, availability, capacity, bandwidth, and redundancy

- Do monitoring tools send notifications when your systems are nearing their capacity?
- If your systems go down for any reason, does the user community get notified?
- Do you have boundary protection—especially important for FedRAMP and PCI DSS certification?
- Are your communications, subnets, interfaces, and communications isolated and
- protected? How?

- Regarding your servers:

  - Do you restrict server communications traffic, both outgoing and incoming?
  - Do outgoing communications meet confidentiality and integrity standards?
  - Are they encrypted? How?
  - Do you have host-based protection?
  - Are your security tools for these servers isolated, too?

- Are your systems configured and protocols enforced for breach protection? Are they dynamically isolated and segregated? Do your FedRAMP and financial systems have separate subnets, network connections, and security domains? Are these systems resilient?
- Do your systems generate notifications when networks get disconnected or disrupted?
- Do they catalogue downtime? What are your processes in case of inactivity?
- How do you secure data? How do privacy attributes get transmitted? Do you use public key infrastructure certificates? Secure socket layering (SSL)?
- Do you use Voice-over IP (VoIP) protocols? If so, how do you secure the data generated?
- How do you secure your system components?
- How do you partition your systems? What are the channels of distributed storage and processing?
- What are your wireless link protocols? Do you have wifi throughout your office? Is it visible? How is it protected? Do you use electromagnetic interference or anti-jam protection?
- If your buildings contain sensors, what data are they capturing, and in what environment? How do you protect that data?
- Are there resets on the use of all devices? How are they configured?
- Do you have malicious code protection on every device—software, hardware, firmware, and entry points?
- Are your internal and external systems monitored for malicious activity? Does the monitoring system generate logs of attacks and attempted intrusions? Who gets notified when this activity occurs? How and when are they notified?

- Do you have continuous monitoring in place for each of the following?

  - Connection problems
  - System outages
  - Unauthorized access to the network
  - Deployment of any device
  - Modification or deletion of any system configuration settings

- What is your incident response program? How is your system intrusion detection system configured? Does it include real-time analysis of system changes or problems? System-generated alerts?
- What kinds of security and privacy verification do you use?
- Do you have memory protection? What kind?

20. System information integrity

What are the integrity policies and procedures for your IT system? Be prepared to show documentation.

- Do you have security controls? What kind?
- What is your process for system information integrity planning and implementation?
- How do you protect devices from malicious code? If a breach occurs, what is the process for corrective action?
- What is the testing and certification process for implementing changes in your system?
- Are remote commands authenticated? How?
- Do you review and analyze traffic and event patterns to spot abnormalities?
- Is there monitoring of:

  - Wireless-to-wireless communications?
  - Host-based devices
  - Network devices?

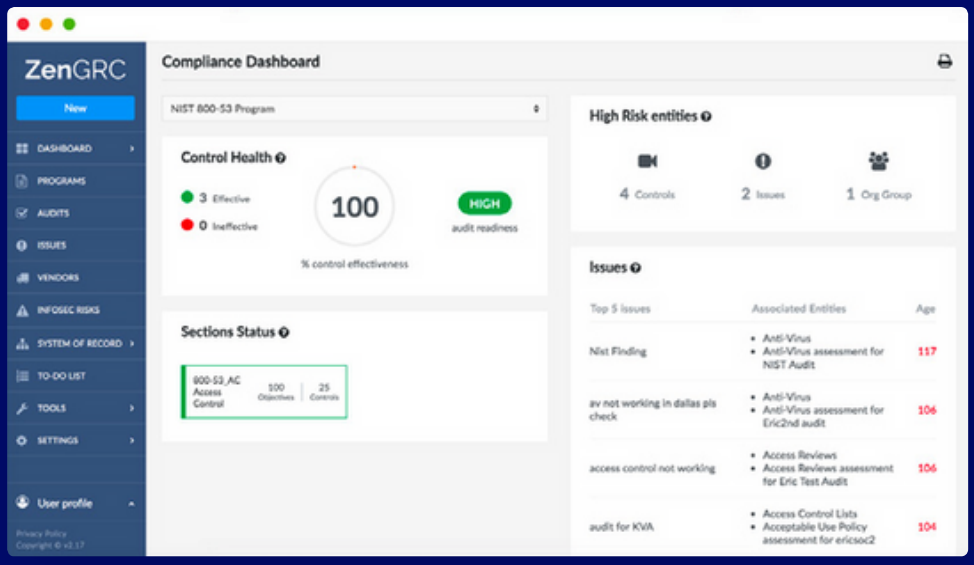
- Are your devices audited?
- Are all devices and network servers tested and approved before use?
- Does monitoring protect user privacy? How?
- Are your integrated systems tracked and monitored regularly?
- Is there spam protection at your systems' entry and exit points? Is it updated regularly using a centrally managed automated process?
- How do you ensure that patches and updates get applied as soon as they become available?
- How do you validate input? Do you use structured messages, prescreening, or syntax validation?
- How do you handle data errors?
- What are your information management and retention policies?
    - How long do you keep data and records?
    - How do you destroy data?
    - What is the approval process for data destruction?
- How do you prevent predictable failures?
- Have you implemented non-persistence for your information security components?
- Do you have fail-safe procedures to determine next steps in case your critical system components lose the ability to communicate? If a communication failure were to occur, how would you alert your IT operators and provide instructions?
- How do you dispose of information, especially PII?
- How do you ensure that PII is:
    - Accurate?
    - Properly classified or tagged?
    - Easy to identify and update?
    - Masked
    - Encrypted?
- What are your disclosure and privacy policies for collecting and processing PII?
- If the owner of PII requests their data, what are your processes for providing it?

Pro-Tip: Don’t Tackle NIST Alone.

Implementing a NIST 800-53 based security framework may be one of the most challenging tasks a compliance or security professional will undertake. But being able to assure clients, customers, and prospects about the security of your systems, your networks, and their data is worth your time and effort.

And NIST guidance will place you in the proverbial driver’s seat when it comes time for other security-related audits such as FedRAMP, SOX, and PCI DSS.

Given NIST's complexity, however, this is one framework you won't want to manage with cumbersome, old-fashioned spreadsheets.



A quality governance, risk, and compliance (GRC) software can help you sail through your NIST audit in a fraction of the time and with much less effort.

No more hunting for documentation; no more searching emails or toggling screens. Centralized dashboards and simplified self-assessments can make aligning to NIST 800-53 a worry-free, Zen-like experience, freeing you and your personnel to focus on the task at hand: keeping your data, systems, and networks secure and operational, and your clients and customers happy.

About ZenGRC

Founded in 2009, ZenGRC offers Simply Powerful GRC solutions through its ZenGRC and ZenGRC Pro products. Renowned for in-house expertise, it ensures comprehensive access to all modules and frameworks, streamlining governance, risk, and compliance management.

Contact a ZenGRC expert today to request your **free demo**, and embark on the worry-free path to regulatory compliance—the Zen way.

www.zengrc.com
engage@ZenGRC.com
(877) 440-7971