

GRC Interview & Study Guide

NIST CSF 2.0 & SP 800-53

Prepared by **Naresh Thalla Mudhiraj** · thallanaresh.com

Personal learning project. Views are my own and do not represent any employer.

Basic to Advanced · scenario-based questions · practical examples · why each topic matters

Version 2.0 · generated 21 October 2026

The NIST Cybersecurity Framework 2.0, the SP 800-53 control catalogue and the Risk Management Framework.

Study material written in plain language. Framework and regulatory details change; always confirm against the official, current publication before relying on them.

NIST CSF 2.0 & SP 800-53

The NIST Cybersecurity Framework 2.0, the SP 800-53 control catalogue and the Risk Management Framework.

Q: What is the NIST Cybersecurity Framework (CSF) 2.0?

Basic

NIST CSF 2.0, released in February 2024, is a voluntary framework that helps organisations of any size or sector understand, assess, prioritise and communicate cybersecurity risk.

- **It is outcome-based:** it says what to achieve, not exactly how.
- Version 2.0 broadened the scope beyond critical infrastructure to all organisations.
- Its core is organised into Functions, Categories and Subcategories, supported by implementation examples and informative references to other standards.

Practical example: A mid-sized US hospital uses CSF 2.0 to describe its current and target security posture to the board, then picks specific controls from CIS Controls and HIPAA to close the gaps.

Why this matters: CSF is a common language for boards and technical teams, and is widely used to structure security programmes and maturity assessments worldwide.

Q: What are the six functions of NIST CSF 2.0?

Basic

- **Govern (GV):** establish and monitor the organisation's cybersecurity risk management strategy, expectations and policy. New in 2.0.
- **Identify (ID):** understand current cybersecurity risks — assets, risk assessment, improvement.
- **Protect (PR):** safeguards to manage risk — identity and access, awareness, data security, platform security, resilience.
- **Detect (DE):** find and analyse possible attacks and compromises.
- **Respond (RS):** take action on a detected incident.
- **Recover (RC):** restore assets and operations affected by an incident.

Govern sits at the centre, informing how the other five are implemented.

Practical example: Govern: the board approves the cyber strategy. Identify: asset inventory. Protect: MFA. Detect: SIEM alerts. Respond: incident playbooks. Recover: restoring from backups and communicating with stakeholders.

Why this matters: Expect this question for almost any GRC role — and mentioning that Govern is new in 2.0 shows you are up to date.

Q: What are the three parts of NIST CSF 2.0 (Core, Profiles, Tiers)?

Basic

- **The CSF Core:** a hierarchy of cybersecurity outcomes arranged as Functions (6), Categories and Subcategories.
- **CSF Organizational Profiles:** a description of an organisation's current and/or target posture in terms of Core outcomes, used to find and prioritise gaps.
- **CSF Tiers:** a way to describe how rigorous the organisation's cybersecurity risk governance and management practices are, from Tier 1 (Partial) to Tier 4 (Adaptive).

NIST also publishes supporting online resources such as Implementation Examples, Informative References and Quick Start Guides.

Practical example: A company records its current profile for PR.AA (identity management, authentication and access control) as partially achieved, sets a target of fully achieved, places itself at Tier 2 overall and aims for Tier 3 within 18 months.

Why this matters: Knowing how the parts fit together lets you use the CSF practically, for assessment and roadmap planning, not just as a list of functions.

Q: What does a CSF subcategory identifier like PR.AA-01 mean?

Basic

- The first part is the Function (PR = Protect).
- The second part is the Category (AA = Identity Management, Authentication, and Access Control).
- The number is the specific Subcategory outcome (01 = identities and credentials for authorised users, services and hardware are managed by the organisation).

CSF 2.0 reorganised many categories compared with 1.1. For example, the old PR.AC was replaced by PR.AA, and the supply chain category moved under Govern as GV.SC.

Practical example: A gap report lists 'PR.AA-03: Users, services, and hardware are authenticated, not met for service accounts' and links it to a project to vault and rotate service-account credentials.

Why this matters: Using identifiers precisely makes mapping, gap assessments and evidence tracking much clearer.

Q: What are the categories under the Govern function in CSF 2.0?

Basic

- **GV.OC Organizational Context:** mission, stakeholder expectations and legal and regulatory requirements.
- **GV.RM Risk Management Strategy:** priorities, constraints, risk appetite and tolerance statements.
- **GV.RR Roles, Responsibilities, and Authorities:** accountability, including leadership's.
- **GV.PO Policy:** establishing, communicating and enforcing cybersecurity policy.
- **GV.OV Oversight:** results of risk management activities are used to inform and adjust strategy.
- GV.SC Cybersecurity Supply Chain Risk Management.

Practical example: For GV.RM, the company documents a board-approved risk appetite statement. For GV.OV, the risk committee reviews KRI results each quarter and changes priorities when ransomware readiness falls behind.

Why this matters: Govern is the biggest change in CSF 2.0 and is where GRC professionals add most value, so interviewers often ask about it in detail.

Q: An executive asks what the six CSF functions mean for their department. How do you explain it simply?

Basic · Scenario

- Use their world, not framework language. For a clinic operations director, for example:
- **Govern:** who decides how much cyber risk the clinics can take, and who is accountable.
- **Identify:** knowing which systems and data the clinics rely on, and what could go wrong.
- **Protect:** the safeguards, such as logins with MFA, trained staff and backups.
- **Detect:** noticing quickly when something is wrong.
- **Respond:** what the clinic does in the first hours of an incident.
- **Recover:** getting back to normal, such as restoring systems and catching up on records.

Then give one concrete action their department owns under each function.

Practical example: For the clinic director, Respond means 'switch to paper downtime forms and call the IT hotline', and Recover means 'enter paper records into the EHR within 24 hours of restoration'. Both are added to the clinic's own checklist.

Why this matters: Translating frameworks into business terms is how GRC professionals win support from non-technical leaders.

Q: What does the Govern function add in CSF 2.0?

Intermediate

Govern elevates cybersecurity governance to a top-level function. Its categories cover:

- Organisational context (mission, stakeholders, legal and regulatory requirements).
- Risk management strategy (priorities, appetite, tolerance).
- Roles, responsibilities and authorities.
- Policy.
- Oversight (reviewing and adjusting the strategy).
- Cybersecurity supply chain risk management.

It reflects the view that cybersecurity is an enterprise risk that leadership must direct, not just an IT activity.

Practical example: Under GV.SC, a company formally defines supplier security requirements and contract clauses, something that sat loosely under Identify in CSF 1.1 and now has explicit governance ownership.

Why this matters: This aligns NIST with how modern GRC functions operate, and with the governance focus of ISO 27001 and regulators.

Q: What are CSF Profiles and Tiers?

Intermediate

- **Profiles:** a Current Profile describes the outcomes an organisation is achieving today; a Target Profile describes the outcomes it wants to achieve. The gap between them drives an action plan. Community Profiles are shared baselines for a sector or use case.
- **Tiers:** describe the rigour of cybersecurity risk governance and management — Tier 1 Partial, Tier 2 Risk Informed, Tier 3 Repeatable, Tier 4 Adaptive.

Tiers are not a maturity certification; organisations choose the tier that fits their risk and resources.

Practical example: A current profile shows DE.CM (continuous monitoring) only partly achieved. The target profile for next year raises it to a fully achieved outcome, and the gap becomes a funded project. Tier 2 → Tier 3 shows the move to repeatable, policy-driven practice.

Why this matters: Current vs Target Profile is a practical way to build and justify a security roadmap.

Q: What is NIST SP 800-53?

Intermediate

NIST Special Publication 800-53 (currently Revision 5) is a comprehensive catalogue of security and privacy controls for information systems and organisations.

- It contains 20 control families, e.g. Access Control (AC), Audit and Accountability (AU), Configuration Management (CM), Contingency Planning (CP), Incident Response (IR), Risk Assessment (RA), System and Communications Protection (SC), and Supply Chain Risk Management (SR), which was added in Rev 5.

- Rev 5 integrated privacy controls into the catalogue and made controls more outcome-focused so they can be used by any organisation, not only US federal agencies.
- Control baselines (Low, Moderate, High, plus a privacy baseline) are published separately in SP 800-53B.

It is mandatory for US federal systems and is the basis of programmes such as FedRAMP; many private organisations use it as a detailed control reference.

Practical example: A US federal contractor selects the Moderate baseline from SP 800-53B, tailors controls such as AC-2 (account management) and documents the implementation in its system security plan.

Why this matters: 800-53 is the most detailed public control catalogue — useful for control design even where it is not mandatory.

Q: How does NIST CSF differ from NIST SP 800-53?

Intermediate

- CSF is a high-level, outcome-based framework for managing and communicating cybersecurity risk. It is concise and voluntary.
- SP 800-53 is a detailed catalogue of specific security and privacy controls and enhancements.
- **They are complementary:** CSF says what outcomes to achieve; 800-53 provides detailed controls that can achieve them. NIST publishes mappings between the two.

Practical example: CSF says 'identities and credentials are managed' (outcome). SP 800-53 says exactly what to implement, such as IA-2(1) multi-factor authentication to privileged accounts (control).

Why this matters: Showing that you know which tool fits which audience (board vs control owners) is a mark of a senior practitioner.

Q: Which other NIST publications are useful for GRC professionals?

Intermediate

- **SP 800-30:** guide for conducting risk assessments.
- **SP 800-37:** Risk Management Framework.
- **SP 800-61:** computer security incident handling guide (Revision 3 aligns incident response with CSF 2.0).
- **SP 800-34:** contingency planning guide for information systems.
- **SP 800-161:** cybersecurity supply chain risk management.
- **SP 800-171:** protecting Controlled Unclassified Information in non-federal systems.
- **NIST Privacy Framework:** a companion to the CSF for privacy risk.

Practical example: Use SP 800-30 to run the risk assessment, SP 800-61 to structure the incident response plan, SP 800-34 for contingency planning and SP 800-161 when assessing software supply chain risk.

Why this matters: Referencing the right guidance for a specific problem shows depth beyond the headline frameworks.

Q: What are CSF Implementation Tiers, and are they a maturity model?

Intermediate

- **Tier 1 Partial:** ad hoc, reactive cybersecurity risk management.
- **Tier 2 Risk Informed:** practices approved by management but not organisation-wide policy.
- **Tier 3 Repeatable:** formally approved, expressed as policy and regularly updated.
- **Tier 4 Adaptive:** adapts based on lessons learned and predictive indicators, and is part of the organisational culture.

NIST says Tiers describe the rigour of risk governance and management practices. They are not meant as a strict maturity model for every subcategory, and not every organisation needs Tier 4. Many organisations still use them, or their own scale, to express maturity.

Practical example: A regional clinic group targets Tier 3 because its risk is significant but its resources are limited. A national bank targets Tier 4 for its threat intelligence and response practices.

Why this matters: Interviewers check you do not over-claim what the Tiers mean and that you choose a target level based on risk and resources.

Q: How do you perform a NIST CSF 2.0 gap assessment?

Intermediate

1. Agree scope and objectives with sponsors (whole enterprise or a business unit).
2. Select the relevant subcategories and consider using a Community Profile for your sector.
3. Collect evidence through interviews, documents and technical data for each outcome.
4. Rate the current state with a consistent scale and record it in a current profile.
5. Agree the target profile with leadership, based on risk, regulation and appetite.
6. Analyse and prioritise the gaps, then build an action plan with owners, cost and timing.
7. Reassess periodically to track progress.

Practical example: The assessment rates 106 subcategories. The biggest gaps are GV.SC (no supplier security requirements) and RC.RP (recovery plans not tested). These become the top two roadmap items, with a board update every quarter.

Why this matters: A CSF assessment is one of the most common GRC deliverables. A structured method makes results defensible and repeatable.

Q: What are the SP 800-53 control families, and what are control enhancements?

Intermediate

SP 800-53 Rev. 5 groups controls into 20 families, such as AC (Access Control), AU (Audit and Accountability), CM (Configuration Management), IR (Incident Response), RA (Risk Assessment), SC (System and Communications Protection), SR (Supply Chain Risk Management) and PT (PII Processing and Transparency).

- A base control states the main requirement (for example AC-2 Account Management).
- Control enhancements add strength or capability, shown in brackets, such as AC-2(1) Automated System Account Management.
- Baselines (Low, Moderate, High and a Privacy baseline) are published in SP 800-53B.
- Rev. 5 made controls outcome-based and integrated privacy and supply chain controls into the main catalogue.

Practical example: A SaaS vendor pursuing FedRAMP Moderate maps its existing ISO 27001 controls to the Moderate baseline and finds it needs extra enhancements in AU (audit log review automation) and CM (baseline configuration).

Why this matters: Federal, defence and many regulated organisations specify requirements in 800-53 terms, so you need to read and map them confidently.

Q: What is FIPS 199 security categorisation?

Intermediate

FIPS 199 categorises information and systems by the potential impact (Low, Moderate, High) of a loss of confidentiality, integrity or availability.

- Each information type gets a rating for C, I and A.
- The system's overall category is usually the highest rating across them (the high-water mark).
- SP 800-60 helps map information types to provisional impact levels.
- The category drives which SP 800-53B baseline applies in the RMF Select step.

Practical example: A benefits system holds personal health information: confidentiality Moderate, integrity Moderate, availability Low. The overall categorisation is Moderate, so the Moderate baseline applies.

Why this matters: Categorisation sets the scale of the control effort. Getting it wrong either wastes money or leaves a system under-protected.

Q: Leadership asks you to 'implement NIST CSF' in a company that already has ISO 27001. What do you advise?

Intermediate · Scenario

- Do not create a second programme. Use the CSF as a lens and communication tool on top of the existing ISMS.
- Map the CSF subcategories to your ISO 27001 Annex A controls and SoA (NIST provides informative references to help).
- Use CSF profiles to show current versus target posture to the board, especially for Govern, Detect, Respond and Recover.
- Close the gaps the mapping reveals, often in supply chain governance, continuous monitoring and recovery testing.
- Report using CSF functions if leadership finds that clearer, while keeping ISO certification evidence in the ISMS.

Practical example: The mapping shows ISO coverage for most Protect outcomes but weak evidence for RC.RP (executing recovery plans). The company adds annual full-recovery exercises and reports progress to the board using a one-page CSF profile.

Why this matters: Avoiding duplication saves money and keeps one source of truth, while gaining the CSF's strength in board communication.

Q: A US customer asks you to show your posture against NIST CSF 2.0 in two weeks. How do you respond?

Intermediate · Scenario

- **Clarify what they need:** a self-assessment, a mapping, or evidence for specific outcomes.
- Use an existing mapping from your current framework (ISO 27001 or SOC 2) to the CSF to produce a profile quickly.
- Be honest about partial areas and include planned improvements with dates.
- Provide supporting evidence such as certificates and SOC 2 reports instead of raw internal documents.
- Keep the result as a reusable asset for other customers.

Practical example: Within 8 days the team sends a 6-page CSF 2.0 profile summary built from its SOC 2 controls mapping, flags two partially met outcomes with remediation dates, and attaches the SOC 2 Type II report under NDA.

Why this matters: Customers increasingly use the CSF as a common language. A quick, honest and reusable response builds trust and saves future effort.

Q: You need to choose a framework for a 200-person healthcare startup with no security programme. NIST CSF, ISO 27001 or CIS Controls?

Intermediate · Scenario

- **Start from the drivers:** customers, regulations (HIPAA in the US, local health rules elsewhere), and what buyers ask for.
- CIS Controls (with their Implementation Groups) give a practical, prioritised technical starting point for a small team.
- NIST CSF 2.0 gives a business-friendly structure and board language, plus the Govern function.
- ISO 27001 gives a certifiable management system that customers recognise, especially outside the US.
- **A common answer:** use CIS IG1 for quick wins, CSF to structure and report, and plan ISO 27001 (or SOC 2) when sales require it.

There is no single correct answer. Interviewers want your reasoning.

Practical example: The startup applies CIS IG1 in the first 6 months (inventory, MFA, backups, patching), reports progress to the board as a CSF profile, and starts ISO 27001 in year two when it bids for hospital contracts abroad.

Why this matters: Framework selection questions test judgement, not memory. Linking the choice to business drivers is what matters.

Q: What are the steps of the NIST Risk Management Framework (RMF)?

Advanced

The RMF (NIST SP 800-37 Rev 2) has seven steps:

1. **Prepare:** establish context and priorities at organisation and system level.
2. **Categorise:** determine system impact level based on the information processed (using FIPS 199 / SP 800-60).
3. **Select:** choose and tailor controls from SP 800-53.
4. **Implement:** put controls in place and document them.
5. **Assess:** determine whether controls are implemented correctly and producing the desired outcome.
6. **Authorise:** a senior official accepts the residual risk and authorises the system to operate (ATO).
7. **Monitor:** continuously monitor controls, changes and risk.

Practical example: For a new claims-processing system: Prepare, Categorize (Moderate under FIPS 199), Select the baseline, Implement, Assess with an independent assessor, Authorize (ATO signed by the authorising official), Monitor continuously.

Why this matters: RMF illustrates the full lifecycle from categorisation to continuous monitoring — a useful model even outside government.

Q: How do NIST SP 800-171 and CMMC relate, and why might they matter outside the US?

Advanced

- SP 800-171 sets security requirements for protecting Controlled Unclassified Information (CUI) in non-federal systems. Revision 3 was published in 2024.
- The US Department of Defense's CMMC programme uses SP 800-171 as the basis for its assessment levels for defence contractors.

- Outside the US, these matter for companies in the defence supply chain or those serving US government clients, including overseas subsidiaries.
- They also offer a useful, well-structured control set for protecting sensitive data in general.

Practical example: An engineering firm outside the US supplying parts to a US defence prime is told it must meet SP 800-171 requirements and prepare for a CMMC assessment before the next contract renewal.

Why this matters: Multinational employers often have US federal or defence customers. Knowing where these requirements come from helps you scope programmes correctly.

Q: How does the NIST AI Risk Management Framework (AI RMF) relate to the CSF?

Advanced

The NIST AI RMF 1.0 (2023) is a voluntary framework for managing risks of AI systems. It has four functions:

- **Govern:** culture, policies, accountability for AI risk.
- **Map:** understand the context and identify risks of an AI system.
- **Measure:** analyse, assess and track AI risks (accuracy, bias, robustness, security).
- **Manage:** prioritise and act on risks.

It complements the CSF. The CSF addresses cybersecurity outcomes, while the AI RMF covers wider trustworthiness issues such as fairness, transparency and safety. NIST has also published a Generative AI profile for the AI RMF.

Practical example: Before deploying an AI tool that summarises clinical notes, the governance group uses the Map function to identify risks such as inaccurate summaries, then Measure to test error rates on sample notes before approving a limited pilot.

Why this matters: AI governance roles are growing quickly. Showing you can connect cyber frameworks with AI risk frameworks is valuable in interviews.

Q: What is continuous monitoring in the RMF, and how is it different from a one-time authorisation?

Advanced

- In the RMF Monitor step, controls and risks are monitored on an ongoing basis according to a continuous monitoring strategy (SP 800-137).
- **Monitoring frequency is based on control volatility and risk:** automated controls might be checked daily, policies yearly.
- Results feed ongoing authorisation decisions, so the authorising official sees current risk instead of a 3-year-old assessment.
- It requires good asset data, automation and clear thresholds for when changes trigger reassessment.

Practical example: Instead of reassessing every 3 years, an agency's system has vulnerability, configuration and account data fed into a dashboard weekly. A significant configuration drift triggers a targeted reassessment rather than waiting for the next cycle.

Why this matters: Point-in-time compliance quickly goes stale. Continuous monitoring is where modern GRC (and CCM tools) is heading.

Q: The authorising official refuses to sign an ATO because of many open POA&M items. What do you do?

Advanced - Scenario

- Review the Plan of Action and Milestones (POA&M) with the system owner and prioritise by risk.

- Close quick wins and get realistic dates and resources for the rest.
- Identify compensating controls that reduce risk while items are open.
- **Present a clear risk picture to the authorising official:** what is open, the residual risk and the plan.
- Options include a time-limited or conditional authorisation, reduced system scope, or delaying go-live. The AO decides; GRC makes sure the decision is informed and documented.

Practical example: Of 34 POA&M items, 12 are closed in two weeks and 8 are covered by compensating monitoring. The AO grants a 6-month authorisation with conditions and a required review of the remaining high items.

Why this matters: The RMF puts risk acceptance in the hands of the authorising official. GRC supports a decision that is evidence-based rather than pushing for a signature.

Q: Your SOC uses NIST SP 800-61, but the new revision aligns incident response to CSF 2.0. How do you update the programme?

Advanced - Scenario

- Read the new revision (SP 800-61 Rev. 3, finalised in 2025), which describes incident response through the CSF 2.0 functions rather than the older four-phase lifecycle.
- **Map your existing plan and playbooks to the CSF functions:** preparation lives largely in Govern, Identify and Protect, while Detect, Respond and Recover cover the incident itself.
- Check gaps such as governance roles, supplier involvement and lessons-learned feedback into risk management.
- Update the plan, train the team and test with a tabletop exercise.
- Keep what works. Revision changes are about alignment and integration, not discarding effective processes.

Practical example: The IR plan update adds a Govern section (decision rights, regulatory notification owners, supplier contacts) and a feedback step that sends lessons learned into the risk register. It is validated in a ransomware tabletop exercise with executives.

Why this matters: Keeping incident response aligned with current guidance shows a living programme. Auditors and customers notice outdated references.