

NIST publications for school districts

A one-stop map of the National Institute of Standards and Technology (NIST) guidance that matters to K-12 leaders and IT teams. Each row says what the publication is for, the reading level and the Cybersecurity Framework (CSF) 2.0 functions it supports: **GV** Govern, **ID** Identify, **PR** Protect, **DE** Detect, **RS** Respond, **RC** Recover. Reading levels: **L** Leader, **P** Practitioner, **T** Technical.

Start here

SUPERINTENDENTS AND CABINET	TECHNOLOGY DIRECTORS	BUSINESS OFFICIALS	IT STAFF AND SERVICE PARTNERS
Lead cybersecurity as a district risk <ol style="list-style-type: none"> SP 1299 Eight pages that explain the framework your rubric is built on. SP 1300 Actions and questions to work through with your cabinet. SP 1303 Put cyber risk on the same list as the district's other risks. IR 8374 Rev. 1 What ransomware readiness requires, function by function. NIST AI 600-1 Risks to weigh before staff and students use generative AI. 	Build the program around CSF 2.0 <ol style="list-style-type: none"> CSF 2.0 (CSWP 29) The structure behind every rubric category. SP 1301 Turn your baseline into Current and Target Profiles. SP 800-61 Rev. 3 Build the incident response plan on current guidance. SP 800-63B-4 Set password and MFA policy that matches NIST today. SP 800-40 Rev. 4 Make patching routine and predictable. 	Budgets, vendors and continuity <ol style="list-style-type: none"> SP 1326 Due diligence before buying or renewing technology. IR 8286D (Update 1) Rank systems by impact to set recovery priorities. SP 800-88 Rev. 2 Wipe devices properly before resale, return or recycling. SP 800-50 Rev. 1 Role-based training for finance and payroll staff. 	Hands-on technical references <ol style="list-style-type: none"> SP 800-63B-4 Password, MFA and passkey requirements. SP 800-177 Rev. 1 Lock down the district email domain with SPF, DKIM and DMARC. SP 1800-25 Inventory and harden assets against ransomware. SP 800-92 Keep logs you can actually investigate with. SP 800-34 Rev. 1 Recovery plans and restores that work.

Start with the framework

CSF 2.0 (CSWP 29) 2024	The NIST Cybersecurity Framework (CSF) 2.0 The common language most cybersecurity guidance now uses: six functions (Govern, Identify, Protect, Detect, Respond, Recover) broken into outcomes any organization can work toward. Every district leader should know its shape, because the Cybersecurity Rubric 2.0 is organized the same way. Read it when you set priorities or explain your program to a board.	L	40m	GV ID PR DE RS RC
SP 1299 2024	NIST Cybersecurity Framework 2.0: Resource and Overview Guide An eight-page tour of CSF 2.0 with one page per function and a map of NIST's companion resources. It is the fastest way for a cabinet member or new technology hire to get oriented. Read it before the full framework.	L	10m	GV ID PR DE RS RC
SP 1300 2024	NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide A practical on-ramp to CSF 2.0 for organizations with little formal security planning, and NIST names schools among its intended readers. It lists actions to consider and questions to ask for each function. Small and rural districts can use it as a first plan.	L	15m	GV ID PR DE RS RC
SP 1301 2024	NIST Cybersecurity Framework 2.0: Quick-Start Guide for Creating and Using Organizational Profiles Explains how to describe where you are (Current Profile) and where you want to be (Target Profile) using CSF outcomes, then close the gap. It is the method behind turning an assessment into a plan. Read it before setting rubric targets.	P	20m	GV ID
SP 1302 2024	NIST Cybersecurity Framework 2.0: Quick-Start Guide for Using the CSF Tiers A three-page guide to the four CSF Tiers, which describe how rigorous an organization's cybersecurity risk practices are, from ad hoc to adaptive. Leaders can use it to talk about how the district manages risk, not just which controls exist.	L	8m	GV
CSF 2.0 online resources web resource	CSF 2.0 Resource Center, Reference Tool, Informative References and Implementation Examples NIST's online home for CSF 2.0: the framework, quick-start guides, profile templates, a searchable reference tool and implementation examples for every outcome. The implementation examples are the most practical piece for districts. Bookmark it rather than saving copies.	P	20m	GV ID PR DE RS RC
SP 1347 2026	NIST Cybersecurity Framework 2.0: Informative References Quick-Start Guide Explains informative references: crosswalks that connect each CSF outcome to sections of other standards, such as SP 800-53 or other control sets. Useful when you need to show how district practices line up with a specific standard.	P	15m	GV ID
CSWP 32 (draft) 2024 (draft)	NIST Cybersecurity Framework 2.0: A Guide to Creating Community Profiles A draft guide to Community Profiles: shared CSF baselines written for a sector, technology or threat that many organizations face. NIST has not published a K-12 Community Profile, so this explains how such a profile would be built. Useful to state associations and consortia.	P	20m	GV
IR 7621 Rev. 1 2016	Small Business Information Security: The Fundamentals A plain-language guide to the basics of information security for small organizations, with worksheets for identifying important information and risks. It predates CSF 2.0 (no Govern function), so pair it with SP 1300. Helpful for very small or rural districts starting from scratch.	L	35m	ID PR DE RS RC
Small Business Cybersecurity Corner (web) web resource	Small Business Cybersecurity Corner NIST's hub of free, plain-language resources for small organizations, organized by topic: phishing, ransomware, MFA, cloud, cyber insurance, incident response and more, plus videos and training. A good place for districts with small teams to find short materials for staff.	L	15m	GV PR

Governance, risk and vendors

SP 1303 2024	NIST Cybersecurity Framework 2.0: Enterprise Risk Management Quick-Start Guide Shows how cybersecurity risk feeds into the organization-wide risk discussions leaders already have about finance, safety and operations. Useful for superintendents and business officials who manage district risk as a whole.	L	15m	GV
SP 800-30 Rev. 1 2012	Guide for Conducting Risk Assessments NIST's standard method for assessing information security risk: identify threats and weaknesses, judge likelihood and impact, and report results leaders can act on. Technology directors use it to make risk assessments repeatable. Read chapter 3 and the likelihood and impact tables first.	P	60m	ID GV
SP 800-39 2011	Managing Information Security Risk: Organization, Mission, and Information System View Describes an organization-wide approach to information security risk: frame it, assess it, respond to it and monitor it, at the leadership, business process and system levels. It is the big-picture companion to SP 800-30. Useful when a district formalizes who decides how much risk is acceptable.	P	45m	GV
SP 1314 2024	NIST Risk Management Framework (RMF) Small Enterprise Quick Start Guide An introduction to NIST's Risk Management Framework for small, under-resourced organizations. It explains the value of the seven RMF steps and how to start, without the depth of SP 800-37. Useful if a partner, grant or state agency uses RMF language.	P	15m	GV ID
SP 1305 2024	NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM) A short guide to managing the cybersecurity risk that comes with vendors and technology products, using the CSF's supply chain category (GV.SC). It is written for organizations as buyers. Districts can use it to shape procurement and vendor reviews.	P	15m	GV
IR 8286 Rev. 1 2025	Integrating Cybersecurity and Enterprise Risk Management (ERM) Explains how cybersecurity risks should flow into the risk picture leaders already manage, using cybersecurity risk registers that roll up into an enterprise risk register. Revision 1 aligns the series with CSF 2.0. It suits superintendents and business officials who want cyber risk discussed alongside other district risks.	P	45m	GV
IR 8286D (Update 1) 2025	Using Business Impact Analysis to Inform Risk Prioritization and Response Shows how a business impact analysis, usually done for continuity planning, can also rank which systems and data deserve the most protection and the fastest recovery. A short, practical read for deciding what matters most when the network is down.	P	25m	GV ID RC
SP 800-221 2023	Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio Extends the risk register approach from cybersecurity to all technology risk, including privacy, supply chain and AI, so separate programs feed one enterprise view. Its short companion, SP 800-221A, lists the outcomes to aim for. Useful for business officials coordinating several technology-related risk areas.	P	45m	GV
SP 800-161 Rev. 1 (Update 1) 2024	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations NIST's comprehensive guide to managing cybersecurity risk from suppliers and technology products, with strategy, policy, plans, risk assessments, controls and templates. It is long and written for large organizations; districts should start with SP 1305 and SP 1326 and use this for depth.	T	60m	GV ID
SP 1326 2026	NIST Cybersecurity Supply Chain Risk Management: Due Diligence Assessment Quick-Start Guide A short guide to researching a supplier or product before buying it or renewing it. It organizes the review around ownership and outside influence, where the product comes from, resilience, basic cyber practices and the vendor's own suppliers. A practical companion to a district vendor review checklist.	P	25m	GV

Protect identities, systems and data

SP 800-63B-4 2025	Digital Identity Guidelines: Authentication and Authenticator Management NIST's current rules for passwords and multi-factor authentication (MFA). It favors long passwords over complex ones, drops forced periodic changes, requires checking new passwords against breached-password lists, and expects phishing-resistant MFA options. Technology directors should read it before setting district password and MFA policy.	P	45m	PR
SP 800-63-4 2025	Digital Identity Guidelines The umbrella volume of NIST's digital identity guidance, covering identity proofing, authentication and federation (single sign-on). It explains how to choose assurance levels based on risk. Read it with SP 800-63B when designing staff, student or family sign-in.	T	40m	PR GV
SP 800-40 Rev. 4 2022	Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology Treats patching as routine preventive maintenance, a normal cost of running technology, rather than an optional security task. It recommends grouping systems, planning for routine and emergency patches, and handling systems that cannot be patched. A short, practical read for technology directors and the business officials who fund maintenance.	P	30m	PR ID
SP 800-88 Rev. 2 2025	Guidelines for Media Sanitization How to make data on laptops, Chromebooks, drives and copiers unrecoverable before reuse, resale or disposal. Revision 2 (2025) replaced Revision 1 and focuses on running a sanitization program with clear roles and verification. Important for districts that refresh 1:1 devices or use e-waste recyclers.	P	30m	PR ID
SP 800-177 Rev. 1 2019	Trustworthy Email How to stop attackers from spoofing your district's email domain and how to protect mail in transit, using SPF, DKIM, DMARC and TLS. Written for email administrators, and usable by small organizations. Read the domain authentication chapter first.	T	45m	PR DE

Protect identities, systems and data

SP 800-46 Rev. 2 2016	Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security How to secure remote access to district systems from home or personal devices: VPNs, portals, remote desktop and direct application access. It advises assuming outside networks are hostile. Useful when staff or contractors reach internal systems from off site.	T	35m	PR
SP 800-124 Rev. 2 2023	Guidelines for Managing the Security of Mobile Devices in the Enterprise How to secure smartphones and tablets that reach district systems, whether district-owned or personal. It catalogs mobile threats and the management tools that address them, such as mobile device management. Useful for districts with staff phones, tablets or student devices under management.	T	40m	PR ID
SP 800-207 2020	Zero Trust Architecture Defines zero trust: no user or device is trusted just because it is on the district network, and every access request is checked. It describes the components and deployment options. Useful as a direction for long-term network and identity planning rather than a product purchase.	T	45m	PR
SP 800-215 2022	Guide to a Secure Enterprise Network Landscape Explains how cloud services and remote users have changed enterprise networks and surveys the security tools now used: cloud access brokers, secure web gateways, next-generation firewalls, microsegmentation and secure access service edge. Helpful when planning a network refresh or E-Rate-funded upgrade.	T	35m	PR
SP 800-41 Rev. 1 2009	Guidelines on Firewalls and Firewall Policy Explains firewall types, what each can and cannot do, and how to write and maintain a firewall policy. It dates from 2009, so product details are old, but the policy principles (deny by default, documented rules, testing) still hold.	T	30m	PR
SP 800-209 2020	Security Guidelines for Storage Infrastructure Security recommendations for storage systems and backups, from file servers and storage arrays to virtualized and cloud storage. A draft Revision 1 (2026) puts more weight on attacks against backups. Useful for IT staff who run district file servers or backup systems.	T	45m	PR RC
SP 1800-25 2020	Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events A practice guide from NIST's National Cybersecurity Center of Excellence on the 'before' side of ransomware: inventory what you have, find weaknesses, and harden assets with secure backups, integrity checks, logging and vulnerability management. Volume A, the executive summary, is short enough for leaders.	T	40m	ID PR
SP 800-213 2021	IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements Helps buyers decide, before purchase, what security capabilities a connected device and its maker must provide. Districts can apply it to cameras, door access, HVAC controls, interactive displays and other connected equipment. Pair it with IR 8259A's baseline of device capabilities.	P	30m	GV PR
IR 8259A 2020	IoT Device Cybersecurity Capability Core Baseline A short list of six security capabilities connected devices should generally have: a unique identity, configurable settings, data protection, restricted interface access, secure software updates and awareness of their own security state. A practical checklist for purchasing.	P	20m	PR GV
SP 800-144 2011	Guidelines on Security and Privacy in Public Cloud Computing Lists the security and privacy issues to weigh before moving data or services to a public cloud provider, from governance and compliance to data protection and incident response. Dated (2011), but its outsourcing questions still fit software-as-a-service decisions.	P	35m	GV PR

Detect and test

SP 800-92 2006	Guide to Computer Security Log Management How to plan and run log management: which logs to collect, how to store and protect them, and how to review them. The final is from 2006; a 2023 draft playbook (Revision 1) gives a shorter, more current planning approach. Useful before buying a log or monitoring service.	T	40m	DE PR
SP 1800-26 2020	Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events A practice guide on the 'during' phase of ransomware and other destructive attacks: spotting, containing and limiting damage to databases, files and configurations as an attack happens. Volume A gives leaders the overview; the other volumes are for technical staff.	T	40m	DE RS
SP 800-94 2007	Guide to Intrusion Detection and Prevention Systems (IDPS) Explains intrusion detection and prevention technologies (network, wireless, behavior analysis and host-based) and how to choose, deploy and run them. It dates from 2007 and a planned revision was retired, so treat product details as background.	T	45m	DE
SP 800-150 2016	Guide to Cyber Threat Information Sharing Explains what threat information is worth sharing, why sharing helps both sides, and how to set up and take part in sharing communities safely. Districts can apply it to K-12 and state sharing groups and to peer networks.	P	30m	ID DE RS
SP 800-115 2008	Technical Guide to Information Security Testing and Assessment How to plan and run technical security tests (reviews, scanning, penetration testing) and turn results into fixes. Its rules-of-engagement template is especially useful when hiring an outside tester. Tool specifics are dated (2008), but the process is sound.	T	40m	ID DE

Respond and recover

SP 800-61 Rev. 3 2025	Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile NIST's current incident response guidance, rewritten in 2025 to fit CSF 2.0. It treats incident response as part of everyday risk management: preparation lives in Govern, Identify and Protect; handling lives in Detect, Respond and Recover. Every district's incident response plan should be built on it.	P	45m	GV ID PR DE RS RC
IR 8374 Rev. 1 2026	Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile The CSF 2.0 outcomes that matter most against ransomware, including data-theft extortion, organized under all six functions. Districts can use it as a ready-made target to measure ransomware readiness and build a response playbook. Revision 1 (2026) replaced the 2022 edition.	P	30m	GV ID PR DE RS RC
Ransomware quick start (2022) 2022	Getting Started with Cybersecurity Risk Management: Ransomware A four-page introduction for leaders on starting ransomware risk management with NIST's ransomware profile. It was written for the 2022 profile, so pair it with IR 8374 Revision 1 for current outcomes.	L	8m	GV RS
Ransomware protection and response (web) web resource	Ransomware Protection and Response NIST's central page for ransomware guidance, linking the ransomware profile, the quick start guide and the three data integrity practice guides. Bookmark it as the starting point for ransomware planning.	L	10m	PR RS RC
SP 800-34 Rev. 1 2010	Contingency Planning Guide for Federal Information Systems The classic guide to writing and maintaining contingency and disaster recovery plans for information systems, including a business impact analysis to set recovery priorities. The templates in its appendices are a practical starting point for districts. Written for federal systems in 2010, it remains NIST's current contingency planning guide.	P	60m	RC ID PR
SP 800-184 2016	Guide for Cybersecurity Event Recovery Focuses on the Recover side: planning recovery inside risk management, building recovery playbooks, learning from past events and measuring recovery. Two worked scenarios (a data breach and destructive malware) make it concrete. Useful for writing the recovery half of an incident response plan.	P	40m	RC ID
SP 1800-11 2020	Data Integrity: Recovering from Ransomware and Other Destructive Events A practice guide on restoring data after it has been corrupted or destroyed by ransomware, other malware, an insider or an honest mistake. It shows a tested lab approach to restoring across typical systems with logging to support investigation.	T	40m	RC PR
SP 800-83 Rev. 1 2013	Guide to Malware Incident Prevention and Handling for Desktops and Laptops How to prevent malware on desktops and laptops and how to handle malware incidents, especially outbreaks across many machines. Written in 2013, before modern ransomware and endpoint detection tools, so use it for the handling process rather than tool advice.	T	30m	PR RS

People, training and workforce

SP 800-50 Rev. 1 2024	Building a Cybersecurity and Privacy Learning Program How to plan, build, run and improve a combined cybersecurity and privacy learning program covering awareness, role-based training and education. It focuses on changing behavior and building culture, with metrics to show whether the program works. The core reference for a district staff training program.	P	45m	PR GV
TN 2276 2023	NIST Phish Scale User Guide A method for rating how hard a phishing email is to recognize, so click and report rates from phishing exercises can be read in context. It explains why a rising click rate may reflect a harder email, not worse staff. Check NIST's license terms before using it in a program.	P	30m	PR
SP 800-181 Rev. 1 2020	Workforce Framework for Cybersecurity (NICE Framework) A shared vocabulary for describing cybersecurity work: tasks, knowledge and skills, grouped into work roles and competency areas. Districts can use it to write job descriptions, plan staff development and talk with partners about coverage. The detailed lists are published separately as NICE Framework Components.	P	25m	GV
SP 1308 2026	NIST Cybersecurity Framework 2.0: Cybersecurity, Enterprise Risk Management, and Workforce Management Quick-Start Guide Connects cybersecurity risk, enterprise risk and staffing decisions, pairing CSF 2.0 with the NICE Workforce Framework. Superintendents and business officials can use it to justify roles, contracts or training based on actual risk.	L	15m	GV
SP 800-12 Rev. 1 2017	An Introduction to Information Security A plain-language primer on information security for people new to the field: principles, roles, threats, policy, risk management and the families of security controls. A good first read for a new technology hire or a cabinet member who wants the basics.	L	60m	GV PR
NICE K12 resources (web) web resource	NICE K12 Cybersecurity Education: Community of Interest, conference and resources NIST's NICE program supports K-12 cybersecurity education and careers: an open community of educators that meets monthly, a national K-12 cybersecurity education conference, and resources for counselors and teachers. This is about teaching students, not securing the district, but many districts connect the two.	L	15m	GV
SP 800-114 Rev. 1 2016	User's Guide to Telework and Bring Your Own Device (BYOD) Security A guide for individual staff rather than IT teams: how to protect personal computers, phones and home networks used for work. Technology directors can borrow from it for staff guidance on working from home or using personal devices.	L	25m	PR

People, training and workforce

Youth security and privacy research (web) web resource	Human-Centered Cybersecurity: Youth Security and Privacy NIST research on how children and teens understand online privacy and security, studied with students, parents and teachers. It includes findings on children's password habits and short videos and posts for parents. Useful background for student digital citizenship and family outreach.	L	15m	PR
--	---	---	-----	----

Privacy and artificial intelligence

Privacy Framework 1.0 (CSWP 10) 2020	NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0 A voluntary framework for managing privacy risk, built to sit alongside the Cybersecurity Framework. It helps districts think about how student and staff data is collected, used and shared, not only how it is secured. Version 1.1 is in draft and aligns with CSF 2.0.	P	40m	GV ID PR
AI RMF 1.0 (NIST AI 100-1) 2023	Artificial Intelligence Risk Management Framework (AI RMF 1.0) A voluntary framework for managing the risks of designing, buying or using AI systems, organized as Govern, Map, Measure and Manage. It describes what makes AI trustworthy, such as being valid, safe, secure, fair, transparent and privacy-enhanced. Useful for districts writing AI guidance or evaluating AI tools.	P	45m	GV ID
NIST AI 600-1 2024	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile Applies the AI Risk Management Framework to generative AI such as chatbots and image generators. It names risks that generative AI creates or makes worse, from confabulated answers to data privacy and information security, and lists suggested actions. A practical companion for district generative AI guidance.	P	40m	GV ID PR
IR 8596 (preliminary draft) 2025 (draft)	Cybersecurity Framework Profile for Artificial Intelligence (Cyber AI Profile): NIST Community Profile An early draft CSF 2.0 Community Profile about two things: securing AI systems and using AI to strengthen cyber defense. It is a preliminary draft released for feedback, so read it for direction, not as settled guidance.	T	40m	GV PR DE

Reference catalogs and specialist guides

SP 800-53 Rev. 5 2020	Security and Privacy Controls for Information Systems and Organizations NIST's comprehensive catalog of security and privacy controls, organized into 20 families from Access Control to Supply Chain Risk Management. Districts rarely implement it directly, but it is the detailed reference behind many frameworks, questionnaires and crosswalks. Look up specific controls rather than reading it cover to cover.	T	60m	GV ID PR DE RS RC
SP 800-53A Rev. 5 2022	Assessing Security and Privacy Controls in Information Systems and Organizations Assessment procedures for every SP 800-53 control, with three methods: examine documents, interview people and test mechanisms. Useful for anyone reviewing evidence, including district teams preparing for an independent review. Read chapter 3 and the method descriptions, not the whole catalog.	T	45m	ID GV
SP 800-53B 2020	Control Baselines for Information Systems and Organizations Ready-made starting sets of SP 800-53 controls for federal systems: low, moderate and high security baselines and a privacy baseline. Districts seldom need it unless a contract specifies a federal baseline.	T	30m	GV PR
SP 800-37 Rev. 2 2018	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy The seven-step Risk Management Framework that federal agencies use to secure and authorize systems: Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor. Most districts will not run the full RMF, but its steps are a sound model for launching a major new system. Use SP 1314 for a short introduction.	T	90m	GV ID
SP 800-218 (SSDF 1.1) 2022	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities A set of secure software development practices for software producers. Districts are buyers, not developers, so its main use is a shared vocabulary for asking edtech and software vendors how they build and patch their products.	T	30m	GV
SP 800-100 2006	Information Security Handbook: A Guide for Managers A management-level overview of the parts of an information security program, from governance and budgeting to incident response. It is dated (2006, corrected 2007) and NIST has begun a revision, so use it for context rather than current practice.	L	60m	GV
SP 800-171 Rev. 3 2024	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations Security requirements that federal agencies place, through contracts or agreements, on organizations that handle Controlled Unclassified Information (CUI). Most districts are not covered, but a federal grant, research partnership or contract could bring it in. Check your agreements before assuming either way.	T	60m	PR GV
SP 800-86 2006	Guide to Integrating Forensic Techniques into Incident Response Practical guidance for IT staff (not law enforcement) on collecting, examining and analyzing data during incident investigations. Tool details are dated (2006), but the core lesson still matters: preserve evidence before wiping systems, and know when to call specialists.	T	40m	RS

Reference catalogs and specialist guides

SP 800-45 Version 2 2007	Guidelines on Electronic Mail Security A 2007 guide to securing self-hosted mail servers and clients. It is still listed as final but predates DMARC and cloud email. Districts on hosted email should use the newer Trustworthy Email guide (SP 800-177) instead.	T	30m	PR
SP 800-210 2020	General Access Control Guidance for Cloud Systems Technical guidance on access control for each cloud service model: infrastructure, platform and software as a service. Most useful to IT staff who administer cloud tenants and their permissions.	T	30m	PR

Match the reading to your rubric gaps

Your weakest Cybersecurity Rubric 2.0 categories point to the right NIST reading.

Rubric 2.0 category	CSF	Start with
Organizational Context	GV.OC	CSF 2.0 (CSWP 29); SP 1299; SP 1301
Risk Management Strategy	GV.RM	IR 8286 Rev. 1; SP 800-30 Rev. 1; SP 1303
Roles, Responsibilities, and Authorities	GV.RR	CSF 2.0 (CSWP 29); SP 1308; SP 800-181 Rev. 1
Policy	GV.PO	CSF 2.0 (CSWP 29); SP 800-12 Rev. 1; Privacy Framework 1.0 (CSWP 10)
Oversight	GV.OV	SP 1303; IR 8286 Rev. 1; SP 1302
Cybersecurity Supply Chain Risk Management	GV.SC	SP 1305; SP 1326; SP 800-161 Rev. 1 (Update 1)
Asset Management	ID.AM	IR 8286D (Update 1); SP 1800-25; SP 800-88 Rev. 2
Risk Assessment	ID.RA	SP 800-30 Rev. 1; SP 800-40 Rev. 4; SP 800-115
Improvement	ID.IM	SP 1301; SP 800-184; SP 800-53A Rev. 5
Identity Management, Authentication, and Access Control	PR.AA	SP 800-63B-4; SP 800-63-4; SP 800-207
Awareness & Training	PR.AT	SP 800-50 Rev. 1; TN 2276; Small Business Cybersecurity Corner (web)
Data Security	PR.DS	SP 800-88 Rev. 2; Privacy Framework 1.0 (CSWP 10); SP 800-209
Platform Security	PR.PS	SP 800-40 Rev. 4; SP 800-177 Rev. 1; SP 800-124 Rev. 2
Technology Infrastructure Resilience	PR.IR	SP 800-34 Rev. 1; SP 800-215; SP 800-207
Continuous Monitoring	DE.CM	SP 800-92; SP 1800-26; SP 800-94
Adverse Event Analysis	DE.AE	SP 800-92; SP 800-150; SP 1800-26
Incident Management	RS.MA	SP 800-61 Rev. 3; IR 8374 Rev. 1; SP 1800-26
Incident Analysis	RS.AN	SP 800-61 Rev. 3; SP 800-86
Incident Response Reporting and Communication	RS.CO	SP 800-61 Rev. 3; SP 800-150
Incident Mitigation	RS.MI	SP 800-61 Rev. 3; SP 1800-26; SP 800-83 Rev. 1
Incident Recovery Plan Execution	RC.RP	SP 800-34 Rev. 1; SP 800-184; SP 1800-11
Incident Recovery Communication	RC.CO	SP 800-184; SP 800-61 Rev. 3

About this guide

Summaries are written in plain language by the K12 Cyber Forward program team for school district leaders and IT staff. Each entry was checked against its official NIST page for the current revision and status, and links go to the official NIST page and DOI. Works written by NIST employees are not subject to copyright in the United States. NIST reserves rights abroad and allows reuse with a citation and the line 'Republished courtesy of the National Institute of Standards and Technology.' Some NIST publications include third-party material that may be under copyright. These summaries are our own words and cite each publication.