Cybersecurity Guidance & Standards Cheat Sheet

Current as of September 28, 2026. Several items are in motion (CIRCIA, CMMC, HIPAA, SSDF); verify status before citing in a deliverable.

Quick Reference

#	Document	Issuer	Binding?	Primary Audience
1	Cybersecurity Framework (CSF) 2.0	NIST	Voluntary	Any organization
2	SP 800-53 Rev 5 (Release 5.2.0)	NIST	Mandatory for federal systems	Federal agencies, FedRAMP, contractors
3	SP 800-37 Rev 2 (RMF) + FIPS 199/200	NIST	Mandatory for federal systems	Federal agencies
4	SP 800-30 Rev 1 (Risk Assessment)	NIST	Voluntary (federal expectation)	Risk assessors
5	SP 800-171 Rev 3	NIST	Contractual (DFARS/CMMC)	Contractors handling CUI
6	SP 800-82 Rev 3 (OT Security)	NIST	Voluntary	ICS/SCADA/OT owners
7	SP 800-61 Rev 3 (Incident Response)	NIST	Voluntary	IR teams
8	SP 800-207 + CISA ZT Maturity Model	NIST / CISA	Federal mandate (OMB M-22-09)	Architects
9	SP 800-63-4 (Digital Identity)	NIST	Mandatory for federal systems	IAM teams
10	SP 800-218 (SSDF)	NIST	Required for federal software suppliers	Software producers
11	SP 800-161 Rev 1 (C-SCRM)	NIST	Voluntary (federal expectation)	Procurement, vendor risk
12	SP 800-40 Rev 4 (Patch Mgmt)	NIST	Voluntary	Operations
13	SP 800-92 / Logging guidance	NIST / OMB / CISA	Mixed	SOC, operations
14	FIPS 140-3 & Post-Quantum FIPS	NIST	Mandatory for federal crypto	Everyone buying crypto
15	AI Risk Management Framework	NIST	Voluntary	AI adopters
16	Cross-Sector CPGs 2.0	CISA	Voluntary	Critical infrastructure
17	CIRCIA	CISA (statute)	Mandatory once final	Critical infrastructure
18	C2M2 v2.1	DOE	Voluntary	Energy, utilities
19	AWIA §1433 + EPA Water Guidance	EPA (statute)	Mandatory (RRA/ERP)	Community water systems
20	AWWA Cybersecurity Guidance	AWWA (industry)	Voluntary	Water/wastewater
21	NERC CIP	NERC / FERC	Mandatory	Bulk electric system
22	TSA Security Directives	TSA	Mandatory	Pipelines, rail
23	CMMC 2.0 / DFARS 252.204-7012	DoD	Contractual	Defense industrial base
24	FedRAMP	GSA / OMB	Mandatory for federal cloud	Cloud providers
25	HIPAA Security Rule	HHS	Mandatory	Healthcare, business associates
26	SEC Cyber Disclosure Rules	SEC	Mandatory	Public companies
27	Federal Cyber Executive Orders	White House	Federal policy	Agencies, suppliers
28	ISA/IEC 62443	ISA / IEC	Voluntary (often contractual)	OT asset owners, integrators, vendors
29	ISO/IEC 27001:2022	ISO / IEC	Voluntary (certifiable)	Any organization
30	CIS Controls v8.1	Center for Internet Security	Voluntary	Any organization

PART 1 - NIST CORE PUBLICATIONS

1. NIST Cybersecurity Framework (CSF) 2.0

Issuer / Version: NIST; CSF 2.0 released February 26, 2024 (replaced CSF 1.1 from 2018).

What it is: A voluntary, outcome-based framework for managing cybersecurity risk. It describes *what* good looks like, not *how* to implement it. It is the common language that most other U.S. frameworks now map to.

Who uses it: Originally written for critical infrastructure, 2.0 explicitly broadens scope to all organizations of any size or sector. Federal agencies, state and local governments, utilities, and private companies all use it as the top-level program structure.

Key contents:

- **Six Functions:** Govern (new in 2.0), Identify, Protect, Detect, Respond, Recover.
- **Govern** pulls strategy, roles, policy, oversight, and supply chain risk management up to the executive level instead of burying them in Identify.
- **Core hierarchy:** Functions -> Categories (22) -> Subcategories (106).
- **Organizational Profiles:** a Current Profile (where you are) and a Target Profile (where you need to be). The gap between them drives the roadmap.
- **Tiers 1-4:** Partial, Risk Informed, Repeatable, Adaptive. Tiers describe rigor of governance and management, not a maturity score for each control.
- **Supplementary resources:** Quick Start Guides (including small business), Implementation Examples, Community Profiles, and Informative References (mappings to 800-53, CIS, ISO, etc.) maintained online in NIST's Cybersecurity and Privacy Reference Tool (CPRT).

How it fits: CSF is the "table of contents." SP 800-53, CIS Controls, ISO 27001, and ISA/IEC 62443 supply the control-level detail. CISA's CPGs 2.0 and NIST SP 800-61 Rev 3 are built directly on CSF 2.0 structure.

Practical notes:

- Best tool for board-level reporting and gap assessments; functions are intuitive for non-technical leaders.
- Not certifiable. Nobody is "CSF compliant"; you are "aligned to" CSF.
- For OT environments, pair with SP 800-82 Rev 3, which applies CSF to OT.
- Migration from 1.1 is mostly re-mapping; watch for subcategories that moved into Govern (e.g., supply chain, roles and responsibilities).

2. NIST SP 800-53 Rev 5 - Security and Privacy Controls

Issuer / Version: NIST; Revision 5 published September 2020. Maintained through patch releases in the CPRT: Release 5.1.1 (November 2023) and Release 5.2.0 (August 27, 2025, focused on software update and patch integrity in response to Executive Order 14306).

What it is: The master catalog of security and privacy controls. Where CSF says "what," 800-53 says "which specific safeguards." It is technology-neutral and applies to any type of system, not just federal IT.

Who uses it: Required for federal information systems under FISMA (excluding national security systems). It is the basis for FedRAMP baselines and is widely used by state governments, utilities, and large enterprises as a reference catalog.

Key contents:

- **20 control families:** AC (Access Control), AT (Awareness & Training), AU (Audit & Accountability), CA (Assessment & Authorization), CM (Configuration Mgmt), CP (Contingency Planning), IA (Identification & Authentication), IR (Incident Response), MA (Maintenance), MP (Media Protection), PE (Physical & Environmental), PL (Planning), PM (Program Mgmt), PS (Personnel Security), PT (PII Processing & Transparency), RA (Risk Assessment), SA (System & Services Acquisition), SC (System & Communications Protection), SI (System & Information Integrity), SR (Supply Chain Risk Mgmt).
- Well over 1,000 controls and enhancements. Each control has the requirement statement, a discussion section, related controls, and optional enhancements.
- **Companion documents:** SP 800-53A (assessment procedures, i.e., how to test each control) and SP 800-53B (Low, Moderate, High, and Privacy baselines).
- **Overlays:** tailored control sets for specific environments, such as the OT overlay in SP 800-82 Rev 3.

How it fits: Operates inside the Risk Management Framework (SP 800-37). You categorize the system (FIPS 199), pick a baseline (800-53B), tailor it, implement, and assess (800-53A).

Practical notes:

- Don't implement it cover-to-cover; start from a baseline and tailor.
- Release 5.2.0 added controls on software update integrity and developer testing (SA-15(13), SA-24, SI-2(7)). Organizations can defer adopting patch releases until the next major release.
- Machine-readable OSCAL, JSON, and spreadsheet formats are available, which makes GRC tooling and crosswalks far easier.
- NIST is developing 800-53 control overlays for securing AI systems.

3. NIST SP 800-37 Rev 2 - Risk Management Framework (RMF), with FIPS 199 and FIPS 200

Issuer / Version: NIST; SP 800-37 Rev 2 (December 2018). FIPS 199 (2004) and FIPS 200 (2006) remain current.

What it is: The federal process for bringing a system from concept to authorized operation and keeping it there. It turns FISMA's legal requirement into a repeatable lifecycle.

Who uses it: All federal agencies, DoD (through DoDI 8510.01), and contractors operating systems on behalf of agencies. Many states and regulated industries borrow it.

Key contents - the 7 steps:

1. **Prepare:** organization- and system-level groundwork (roles, risk strategy, asset inventory). Added in Rev 2.
2. **Categorize:** assign Low/Moderate/High impact for Confidentiality, Integrity, and Availability using **FIPS 199**. The highest rating sets the overall level (the "high-water mark"). SP 800-60 helps map information types.
3. **Select:** choose the 800-53B baseline and tailor it. **FIPS 200** sets the minimum security requirements that trigger baseline selection.
4. **Implement:** deploy controls and document them in the System Security Plan (SSP).
5. **Assess:** independent testing per 800-53A; results go in the Security Assessment Report (SAR).
6. **Authorize:** the Authorizing Official accepts residual risk and issues an Authorization to Operate (ATO). Open findings go into a Plan of Action & Milestones (POA&M).
7. **Monitor:** continuous monitoring per SP 800-137; ongoing authorization.

How it fits: RMF is the process; 800-53 is the content; CSF is the enterprise view. Rev 2 explicitly integrates privacy, supply chain risk, and CSF alignment.

Practical notes:

- The authorization package (SSP, SAR, POA&M) is the deliverable auditors and AOs actually look at.
- The Prepare step is what most programs skip, and it's where they struggle later (unclear boundaries, missing inventories).
- For OT systems, availability is usually the driving impact category, which differs from typical IT systems where confidentiality dominates.

4. NIST SP 800-30 Rev 1 - Guide for Conducting Risk Assessments

Issuer / Version: NIST; Revision 1 (September 2012). Still current. Companion to SP 800-39 (Managing Information Security Risk).

What it is: The standard methodology for conducting cybersecurity risk assessments. It defines risk as a function of threat, vulnerability, likelihood, and impact, and gives a repeatable process to evaluate it.

Who uses it: Federal agencies (it underpins the RA family in 800-53), auditors, and consultants performing formal risk assessments. It is frequently cited in HIPAA risk analyses and state regulations.

Key contents:

- **Three risk tiers (from SP 800-39):** Tier 1 Organization, Tier 2 Mission/Business Process, Tier 3 Information System.
- **Four-step process:** Prepare for the assessment; Conduct the assessment; Communicate results; Maintain the assessment.
- **Conduct phase tasks:** identify threat sources, identify threat events, identify vulnerabilities and predisposing conditions, determine likelihood, determine impact, determine risk.
- **Extensive appendices:** taxonomies of threat sources (adversarial, accidental, structural, environmental), example threat events, assessment scales (Very Low to Very High), and templates.
- Supports qualitative, semi-quantitative, and quantitative approaches.

How it fits: Feeds the RMF Categorize/Select/Authorize steps and CSF's Identify function (ID.RA). Also a useful complement to sector-specific methods like AWWA J100 (RAMCAP) used for AWIA risk and resilience assessments.

Practical notes:

- The appendix tables are the most reused part. They're good for building a consistent scoring rubric across clients.
- It is dated in places (predates cloud-native and modern ransomware economics), but the logic holds.
- For enterprise-level risk aggregation, look at NIST IR 8286 series (integrating cybersecurity with Enterprise Risk Management).

5. NIST SP 800-171 Rev 3 - Protecting Controlled Unclassified Information (CUI)

Issuer / Version: NIST; Revision 3 (May 2024), with SP 800-171A Rev 3 (assessment procedures). SP 800-172 covers enhanced requirements for high-value CUI.

What it is: Security requirements for protecting CUI when it resides on nonfederal systems, meaning contractors, universities, and state/local partners.

Who uses it: Defense contractors (through DFARS 252.204-7012 and CMMC), and increasingly civilian agency contractors. A government-wide FAR CUI rule was proposed in January 2025.

Key contents:

- **Rev 3:** 97 requirements across 17 families, derived from the 800-53 Moderate baseline. Rev 2 had 110 requirements in 14 families.
- Rev 3 introduces **Organization-Defined Parameters (ODPs)** so agencies can set values such as timeframes and frequencies.
- New families in Rev 3 include Planning, System & Services Acquisition, and Supply Chain Risk Management.
- Required artifacts: System Security Plan and Plan of Action.

How it fits: 800-171 is essentially a tailored subset of 800-53 for nonfederal systems. CMMC Level 2 is an assessment of 800-171 compliance.

Practical notes:

- **Version trap:** DoD has kept DFARS and CMMC Level 2 tied to **Rev 2 (110 requirements)** for now. Check the actual contract language before you build to Rev 3.
- Scoping is the biggest cost driver. An enclave approach to shrink the CUI boundary usually beats trying to make the whole enterprise compliant.
- The SPRS score (for DoD) is calculated against Rev 2's 110 requirements.

6. NIST SP 800-82 Rev 3 - Guide to Operational Technology (OT) Security

Issuer / Version: NIST; Revision 3 (September 2023). Retitled from "ICS Security" to "OT Security."

What it is: The primary U.S. government guide for securing industrial control systems and broader OT, including SCADA, DCS, PLCs, building automation, physical access control, and transportation systems. It addresses the unique performance, reliability, and safety requirements of OT.

Who uses it: Utilities (water, wastewater, electric, gas), manufacturing, pipelines, and any organization with cyber-physical systems. It is often the first document regulators and auditors reference for OT.

Key contents:

- **OT overview:** architectures, components, and how OT differs from IT (availability and safety first, long lifecycles, legacy protocols, limited patching windows).
- **OT cybersecurity program development:** governance, business case, cross-functional teams (engineering plus IT security).
- **Risk management for OT:** safety and physical-consequence considerations layered onto the RMF.
- **OT security architecture:** defense in depth, network segmentation, DMZs, zones and conduits concepts, remote access, and dual-homing risks.
- **Applying CSF to OT:** walks CSF functions with OT-specific considerations.
- **Appendix F OT overlay:** tailors the 800-53 Low/Moderate/High baselines for OT and flags controls that need OT-specific implementation or compensating controls.
- Threat sources, vulnerabilities, and summaries of historical incidents.

How it fits: Bridges CSF and 800-53 into the OT world and aligns conceptually with ISA/IEC 62443. It pairs naturally with CISA CPGs 2.0 and DOE C2M2.

Practical notes:

- The OT overlay is the most actionable piece for control selection and for defending compensating controls to auditors.
- It is guidance, not a certification scheme. Use 62443 when you need vendor and component requirements or certification.
- Strong reference for AWIA risk and resilience assessments and emergency response plans on the cyber side.

7. NIST SP 800-61 Rev 3 - Incident Response Recommendations

Issuer / Version: NIST; Revision 3 (April 2025). Rev 2 (2012) is withdrawn.

What it is: Guidance for integrating incident response into overall cybersecurity risk management. Rev 3 is formally a **CSF 2.0 Community Profile**, not a standalone IR handbook.

Who uses it: SOCs, IR teams, CISOs, and anyone writing an incident response plan or policy.

Key contents:

- **Replaces the classic four-phase lifecycle** (Preparation; Detection & Analysis; Containment, Eradication & Recovery; Post-Incident Activity) with a model mapped to the CSF 2.0 functions:
  - **Govern, Identify, Protect** support preparation and reduce incident frequency and impact.
  - **Detect, Respond, Recover** are the active incident phases.
  - **Improvement** (lessons learned) feeds back continuously across all functions, not just at the end.
- Maps IR considerations to specific CSF subcategories, with recommendations and notes for each.
- Emphasizes roles beyond the security team: legal, communications, leadership, third parties, and service providers.
- Points to external resources for detailed technical procedures rather than embedding them.

How it fits: Aligns IR with CSF 2.0 and CISA CPGs. Supports regulatory reporting timelines (CIRCIA 72 hours, SEC 4 business days, DFARS 72 hours).

Practical notes:

- Many organizations still use the Rev 2 lifecycle in their plans and playbooks. That's fine operationally, but map it to Rev 3 for audits.
- Rev 3 is less "how-to" than Rev 2. For playbook detail, use the CISA Federal Incident & Vulnerability Response Playbooks and SANS resources.
- For OT incidents, supplement with SP 800-82 Rev 3 and CISA ICS guidance; containment in OT must consider safety and process impact.

8. NIST SP 800-207 - Zero Trust Architecture, with the CISA Zero Trust Maturity Model

Issuer / Version: NIST SP 800-207 (August 2020); NIST SP 1800-35 practice guide (2025, 19 example implementations); CISA Zero Trust Maturity Model v2.0 (April 2023). Federal mandate via OMB M-22-09 (January 2022).

What it is: The reference definition of Zero Trust. No implicit trust is granted based on network location; every access request is authenticated, authorized, and continuously evaluated.

Who uses it: Federal agencies (mandated), and enterprises modernizing identity, network, and cloud security.

Key contents (SP 800-207):

- **Seven tenets:** all data sources and services are resources; all communication is secured regardless of location; access is granted per session; access is determined by dynamic policy; asset integrity is monitored; authentication and authorization are dynamic and strictly enforced; telemetry is collected to improve posture.
- **Logical components:** Policy Engine (decides), Policy Administrator (executes), Policy Enforcement Point (gates the connection).
- **Deployment approaches:** enhanced identity governance, micro-segmentation, and software-defined perimeters.

CISA ZTMM v2.0:

- **Five pillars:** Identity, Devices, Networks, Applications & Workloads, Data.
- **Cross-cutting capabilities:** Visibility & Analytics, Automation & Orchestration, Governance.
- **Maturity stages:** Traditional -> Initial -> Advanced -> Optimal.

How it fits: An architecture strategy, not a control catalog. Implemented through 800-53 controls, 800-63 identity assurance, and segmentation practices. CPGs 2.0 added zero trust-related goals.

Practical notes:

- ZT is a journey; ZTMM is the best tool for roadmapping and progress reporting.
- **OT caution:** full ZT enforcement can break deterministic control traffic. In OT, apply ZT principles primarily at remote access, the IT/OT boundary, and engineering workstations, not on Level 0-1 device traffic.
- SP 1800-35 is valuable for seeing real vendor-built reference architectures.

9. NIST SP 800-63-4 - Digital Identity Guidelines

Issuer / Version: NIST; Revision 4 finalized in 2025 (first full update since 2017). Four volumes: 800-63 (overview/risk), 63A (enrollment and identity proofing), 63B (authentication), 63C (federation).

What it is: Requirements for identity proofing, authentication, and federation for systems that interact with users over networks.

Who uses it: Required for federal agencies; the de facto reference for private-sector IAM, SSO, and MFA design.

Key contents:

- **Three assurance dimensions:**
  - **IAL** (Identity Assurance Level 1-3): how confident you are that a person is who they claim.
  - **AAL** (Authenticator Assurance Level 1-3): strength of the login.
  - **FAL** (Federation Assurance Level 1-3): strength of SSO assertions.
- **Password guidance (63B):**
  - Favor length over complexity.
  - Do not impose composition rules or forced periodic rotation.
  - Screen new passwords against breached and commonly used lists.
  - Longer minimums when a password is the only factor.
- **Phishing resistance:** phishing-resistant authenticators are required at AAL3 and must be offered as an option at AAL2. Rev 4 addresses syncable authenticators (passkeys).
- Stronger attention to equity, usability, fraud, and digital injection attacks (deepfakes) in remote proofing.

How it fits: Implements the IA and AC families of 800-53 and supports Zero Trust's identity pillar.

Practical notes:

- The most useful single reference for defending modern password policy against legacy "90-day rotation" audit findings.
- When selecting SSO or MFA platforms, map features to AAL and FAL levels.
- Push-notification MFA without number matching is not phishing-resistant. Plan for FIDO2/WebAuthn or PKI for privileged and remote access.

10. NIST SP 800-218 - Secure Software Development Framework (SSDF)

Issuer / Version: NIST; SSDF v1.1 (February 2022). Executive action in 2025 (EO 14306) directed NIST to update it; check CSRC for the current revision status.

What it is: A core set of high-level secure development practices that can be integrated into any SDLC (waterfall, agile, DevOps).

Who uses it: Software producers, especially those selling to the federal government. It is the basis for the CISA **Secure Software Development Attestation Form** required under OMB M-22-18 and M-23-16.

Key contents - four practice groups:

- **PO - Prepare the Organization:** roles, training, toolchains, security requirements for software.
- **PS - Protect the Software:** protect code from tampering, provide integrity verification (signing), archive releases.
- **PW - Produce Well-Secured Software:** threat modeling, secure design, reuse of vetted components, code review, testing, secure default configurations.
- **RV - Respond to Vulnerabilities:** identify, assess, remediate, and root-cause vulnerabilities; coordinated disclosure.

Each practice includes tasks, notional implementation examples, and references to other standards (such as BSIMM, OWASP SAMM, and ISA/IEC 62443-4-1).

How it fits: Ties to 800-53 SA family controls (reinforced by Release 5.2.0), SBOM efforts, and CISA's Secure by Design initiative.

Practical notes:

- Useful as a **procurement question set** for OT and SCADA vendors: ask them to attest to SSDF or 62443-4-1.
- SP 800-218A adds practices for generative AI and dual-use foundation models.

11. NIST SP 800-161 Rev 1 - Cybersecurity Supply Chain Risk Management (C-SCRM)

Issuer / Version: NIST; Revision 1 (May 2022, updated November 2024).

What it is: Guidance for identifying, assessing, and mitigating risks from suppliers, products, and services throughout their lifecycle.

Who uses it: Federal agencies (required under the SECURE Technology Act and FASCSA), and enterprises managing vendor and product risk, including OT vendors and integrators.

Key contents:

- **Multilevel approach:** enterprise (strategy and policy), mission/business (program-level), and operational (system-level) C-SCRM.
- C-SCRM strategy, policies, plans, and risk assessment templates.
- Supplier criticality analysis: which suppliers can hurt you most.
- Tailored C-SCRM controls built from the 800-53 SR family and related controls.
- Guidance on SBOMs, provenance, counterfeit prevention, and acquisition language.
- Appendices with scenario-based threat examples and templates.

How it fits: Implements CSF 2.0's Govern supply chain category (GV.SC) and the 800-53 SR family. Complements SSDF on the software side.

Practical notes:

- For utilities, the highest-value use is **contract language**: remote access terms, vulnerability disclosure, patch support timelines, SBOM delivery, and incident notification by integrators and vendors.
- Third-party remote access into SCADA environments is one of the most exploited vectors in water sector incidents, so it deserves the most attention.
- The templates are long; scale down for small organizations.

12. NIST SP 800-40 Rev 4 - Enterprise Patch Management Planning

Issuer / Version: NIST; Revision 4 (April 2022).

What it is: Guidance that reframes patching as **preventive maintenance** and an investment in availability, rather than an ad hoc security chore.

Who uses it: IT and OT operations, vulnerability management teams, and CISOs building patch policy.

Key contents:

- The business case for patching, framed around downtime and risk rather than compliance.
- **Risk responses** when a patch can't or shouldn't be applied: accept, mitigate (compensating controls), transfer, or avoid (retire).
- **Maintenance groups:** organize assets by how and when they can be patched, with routine vs. emergency schedules.
- Asset lifecycle management, including planning for end-of-life software.
- Metrics for measuring patch program effectiveness.
- Companion: SP 1800-31 practical implementation guide.

How it fits: Supports 800-53 SI-2 (flaw remediation) and CM controls. Operationally paired with the **CISA Known Exploited Vulnerabilities (KEV) catalog**. BOD 22-01 requires federal agencies to remediate KEV entries within set deadlines, and it's a strong prioritization tool for everyone else.

Practical notes:

- The "maintenance groups" concept maps well to OT: patch HMIs and historians on a scheduled outage cycle, and use compensating controls (segmentation, allow-listing) for PLCs and controllers that can't be patched.
- For OT specifically, also see ISA/IEC 62443-2-3 (patch management in the IACS environment).
- Prioritize by exploitation (KEV, EPSS), not CVSS alone.

13. Logging Guidance - NIST SP 800-92, OMB M-21-31, and CISA Event Logging Best Practices

Issuer / Version:

- NIST SP 800-92 (2006), with a draft Rev 1 "Cybersecurity Log Management Planning Guide" (2023).
- OMB M-21-31 (August 2021).
- Joint CISA and international partner "Best Practices for Event Logging and Threat Detection" (2024).

What it is: Guidance on what to log, how long to retain it, and how to manage it for detection and investigation.

Who uses it: SOCs, IT and OT operations, and federal agencies (M-21-31 is mandatory for them).

Key contents:

- **SP 800-92 (and draft Rev 1):** log management infrastructure, planning, policy, and roles. The draft Rev 1 reframes around planning log management at the enterprise level.
- **OMB M-21-31:** event logging maturity tiers EL0 (not effective) through EL3 (advanced), with specific log types, retention (generally 12 months active storage plus 18 months cold storage), and centralized access requirements.
- **CISA joint guidance:** enterprise-approved logging policy, centralized collection and correlation, secure storage and integrity, detecting living-off-the-land techniques, and OT logging considerations.

How it fits: Implements the 800-53 AU family and CSF Detect (DE.CM, DE.AE). Critical for meeting incident reporting obligations; you can't report what you can't see.

Practical notes:

- Use M-21-31 as a benchmark for retention and log-source coverage even outside government.
- In OT, collect from historians, HMIs, engineering workstations, firewalls at the IT/OT boundary, and remote access gateways. Passive network monitoring fills gaps where devices can't log.
- Prioritize identity and remote access logs; they drive most investigations.

14. Cryptography - FIPS 140-3 and Post-Quantum FIPS 203/204/205

Issuer / Version: NIST.

- FIPS 140-3 (effective 2019; validations via the Cryptographic Module Validation Program, CMVP). FIPS 140-2 certificates were scheduled to move to the historical list in September 2026.
- FIPS 203, 204, and 205 (August 2024): the first post-quantum cryptography standards.

What it is:

- **FIPS 140-3:** requirements and testing for cryptographic modules (hardware, software, firmware).
- **PQC FIPS:** new algorithms resistant to quantum attack.

Who uses it: Mandatory for federal use of cryptography protecting sensitive information. Commonly required by FedRAMP, CMMC (FIPS-validated crypto for CUI), healthcare, and financial sectors.

Key contents:

- **FIPS 140-3:** four security levels (1-4) with increasing physical and logical protections. Aligned with ISO/IEC 19790 and 24759.
- **FIPS 203 (ML-KEM):** key encapsulation (derived from CRYSTALS-Kyber).
- **FIPS 204 (ML-DSA):** digital signatures (CRYSTALS-Dilithium).
- **FIPS 205 (SLH-DSA):** stateless hash-based signatures (SPHINCS+).
- NIST IR 8547 (draft) outlines a transition timeline to deprecate and then disallow quantum-vulnerable algorithms (RSA, ECC) over roughly the next decade.

How it fits: Supports 800-53 SC-13 (cryptographic protection) and IA controls.

Practical notes:

- "FIPS-validated" (has a CMVP certificate) is not the same as "FIPS-compliant" (uses approved algorithms). Contracts usually mean validated.
- With 140-2 certificates going historical, recheck vendor certificates in procurement and audit evidence.
- Start a **cryptographic inventory** now; it is the prerequisite for PQC migration. OT devices with hard-coded crypto will be the long tail.

15. NIST AI Risk Management Framework (AI RMF 1.0)

Issuer / Version: NIST; AI RMF 1.0 (January 2023); Generative AI Profile NIST AI 600-1 (July 2024).

What it is: A voluntary framework for managing risks from designing, developing, deploying, and using AI systems, including trustworthiness, bias, safety, security, and privacy.

Who uses it: Organizations adopting or building AI, including AI-enabled monitoring and analytics tools.

Key contents:

- **Four functions:** Govern (culture, policies, accountability), Map (context and risk identification), Measure (analysis, testing, metrics), Manage (prioritize and respond to risks).
- **Trustworthiness characteristics:** valid and reliable; safe; secure and resilient; accountable and transparent; explainable and interpretable; privacy-enhanced; fair with harmful bias managed.
- **AI RMF Playbook:** suggested actions for each subcategory.
- **GenAI Profile (600-1):** risks unique to generative AI, such as confabulation, data leakage, and information integrity.

How it fits: Parallel to CSF for AI-specific risk. Security of AI systems ties back to 800-53 (AI overlays in development) and SSDF (800-218A).

Practical notes:

- Relevant as vendors add AI features to OT monitoring, SIEM, and anomaly detection. Ask what data leaves the environment and how model outputs are validated before driving operational decisions.
- Useful for writing an acceptable-use and AI governance policy for clients.

PART 2 - CISA, DOE, AND SECTOR-SPECIFIC GUIDANCE

16. CISA Cross-Sector Cybersecurity Performance Goals (CPGs) 2.0

Issuer / Version: CISA; CPG 2.0 released December 2025 (replaced CPG 1.0 from 2022 and 1.0.1 from 2023). CISA is also publishing Sector-Specific Goals (SSGs).

What it is: A prioritized, voluntary subset of IT and OT cybersecurity practices with high risk-reduction value. It answers the question "where do I start?" for small and mid-sized critical infrastructure organizations.

Who uses it: Critical infrastructure owners and operators of all sizes. It's especially useful for resource-constrained utilities. Banking regulators list it as an alternative after sunsetting the FFIEC Cybersecurity Assessment Tool.

Key contents:

- **Aligned to CSF 2.0**, including a new Govern component emphasizing leadership accountability.
- **New and expanded goals** on third-party risk, zero trust architecture, and incident response.
- Each goal includes the risk it addresses, the recommended action, and implementation guidance, with **implementation scales** in 2.0.
- Covers core hygiene: asset inventory, MFA, unique credentials, patching of known-exploited vulnerabilities, logging, backups, segmentation of OT, and incident planning.

How it fits:

- A subset of CSF, and a practical baseline before tackling 800-53 or 62443.
- CISA's free **CSET** tool includes a CPG 2.0 module and checklist.
- CISA's free vulnerability scanning and assessment services map findings to CPGs.

Practical notes:

- The best "first assessment" framework for small water and wastewater utilities. It's short enough to complete in a workshop and credible with boards.
- Many federal grant programs (such as the State and Local Cybersecurity Grant Program) reference CPGs.
- Watch for a water/wastewater Sector-Specific Goals set; CISA has been working with that sector.

17. CIRCIA - Cyber Incident Reporting for Critical Infrastructure Act

Issuer / Version: Statute signed March 2022. CISA proposed rule (NPRM) April 2024. The final rule has slipped from the October 2025 statutory deadline, to May 2026, and then to a **September 2026 target**. It will add 6 CFR Part 226.

What it is: A mandatory federal requirement for covered critical infrastructure entities to report cyber incidents and ransom payments to CISA.

Who uses it: Entities across the 16 critical infrastructure sectors meeting size-based or sector-based criteria. CISA estimates over 300,000 entities will be covered.

Key contents (as proposed):

- **72 hours** to report a "covered cyber incident" after reasonably believing it occurred.
- **24 hours** to report a ransom payment.
- Supplemental reports when substantial new information becomes available.
- Data preservation requirements for incident-related information.
- **Covered-entity criteria:** exceed SBA small-business size standards, OR meet sector-specific criteria. For water, the NPRM covered community water systems and wastewater treatment systems serving more than 3,300 people.
- Exception where a "substantially similar" report is made to another federal agency under an information-sharing agreement.
- Enforcement through requests for information, subpoenas, and referral.

How it fits: Drives IR plans (SP 800-61 Rev 3) and overlaps with SEC, DFARS, TSA, HIPAA, and state reporting obligations.

Practical notes:

- Treat the NPRM as the planning baseline; the final text may change definitions and scope.
- Build a **reporting decision tree** into IR playbooks now, with a 72-hour and a 24-hour clock and a named decision owner.
- Map all overlapping reporting timelines in one matrix to avoid conflicting disclosures.
- Voluntary reporting to CISA (cisa.gov/report) is encouraged before the rule takes effect.

18. DOE Cybersecurity Capability Maturity Model (C2M2) v2.1

Issuer / Version: U.S. Department of Energy; Version 2.1 (June 2022).

What it is: A maturity model for evaluating and improving cybersecurity capabilities across IT and OT. Unlike CSF, it assigns measurable **maturity indicator levels**.

Who uses it: Designed for the energy sector (electric, oil and gas), but it's sector-neutral and widely used by water utilities and other OT-heavy organizations.

Key contents:

- **10 domains:**
  - Asset, Change, and Configuration Management (ASSET)
  - Threat and Vulnerability Management (THREAT)
  - Risk Management (RISK)
  - Identity and Access Management (ACCESS)
  - Situational Awareness (SITUATION)
  - Event and Incident Response, Continuity of Operations (RESPONSE)
  - Third-Party Risk Management (THIRD-PARTIES)
  - Workforce Management (WORKFORCE)
  - Cybersecurity Architecture (ARCHITECTURE)
  - Cybersecurity Program Management (PROGRAM)
- **Maturity Indicator Levels:** MIL0 (not performed), MIL1 (initiated, ad hoc), MIL2 (performed, documented), MIL3 (managed, with governance and resourcing).
- About 350 practices, each tied to a domain and MIL.
- **Free self-evaluation tool** from DOE, which produces a scored report and dashboards. Facilitated evaluations are available.

How it fits: Maps to CSF 2.0 and is complementary to CPGs. CPGs are a baseline; C2M2 is a progression model.

Practical notes:

- An excellent consulting engagement structure: facilitated one- to two-day workshop, scored baseline, target MILs by domain, and a roadmap.
- Most small utilities target MIL1 across all domains first, then MIL2 in priority domains (ASSET, ACCESS, RESPONSE, ARCHITECTURE).
- The results give boards a simple heat map.

19. America's Water Infrastructure Act (AWIA) §1433 and EPA Water Cybersecurity Guidance

Issuer / Version: AWIA (October 2018) amended Safe Drinking Water Act §1433. EPA administers it.

What it is: A mandatory requirement for community water systems serving more than 3,300 people to conduct a **Risk and Resilience Assessment (RRA)** and an **Emergency Response Plan (ERP)**, certify both to EPA, and review and update every five years.

Who uses it: Community drinking water systems. (Wastewater is not covered by §1433.)

Key contents:

- **RRA must assess:** malevolent acts and natural hazards; pipes, physical barriers, source water, treatment, storage, and distribution; **electronic, computer, and automated systems (including security)**; monitoring practices; financial infrastructure; chemical storage and handling; and operation and maintenance.
- **ERP** is due within six months of RRA certification. It must include strategies to improve resilience including cybersecurity, emergency plans and procedures, mitigation actions, and detection strategies.
- **Staggered deadlines by population served** (>=100,000; 50,000-99,999; 3,301-49,999). The second five-year cycle runs 2025-2026.
- Systems must coordinate with local emergency planning committees.

EPA and federal support resources:

- EPA RRA and ERP templates, and the Vulnerability Self-Assessment Tool (VSAT).
- EPA Water Cybersecurity Assessment Tool and free cybersecurity assessments for water systems.
- EPA/CISA "Top Cyber Actions for Securing Water Systems" (2024).
- EPA enforcement alert on water system cybersecurity (May 2024).
- **History:** EPA's March 2023 memo requiring cyber in state sanitary surveys was withdrawn in October 2023 after litigation. Cyber regulation for water remains mainly through AWIA and state action.

Practical notes:

- The RRA's electronic and automated systems section is where cyber consultants plug in. AWWA J100 and SP 800-82 support the methodology.
- The ERP is a natural place to embed cyber incident playbooks, including manual operations procedures if SCADA is lost.
- Certifications attest completion; EPA does not approve content, but EPA can inspect and enforce.

20. AWWA Water Sector Cybersecurity Guidance and Assessment Tool (Industry)

Issuer / Version: American Water Works Association (industry association, not government). The guidance and tool are updated periodically; related standards include ANSI/AWWA J100 (RAMCAP risk and resilience) and G430 (security practices for operations and management).

What it is: A sector-specific, prioritized set of cybersecurity controls for water and wastewater utilities. It is recognized by EPA as a voluntary approach supporting AWIA compliance.

Who uses it: Drinking water and wastewater utilities of all sizes, and the consultants who assess them.

Key contents:

- **Use-case driven:** the utility answers questions about how it uses technology (remote access, mobile devices, SCADA architecture, cloud services). The tool then generates a **prioritized list of controls** relevant to that profile.
- Controls are prioritized in tiers (highest priority first) and **mapped to NIST CSF**, which makes it easy to translate into CSF-based reporting.
- Covers governance, asset management, network architecture, remote access, account management, SCADA security, incident response, and business continuity.
- **J100:** a risk methodology (threat, vulnerability, consequence) used for AWIA RRAs, including malevolent acts such as cyberattacks.

How it fits: Water-sector implementation layer over CSF. Pairs with CPGs 2.0 (baseline), C2M2 (maturity), and SP 800-82 (OT technical depth).

Practical notes:

- The most familiar framework for water utility managers and operators, which lowers resistance compared with NIST-heavy approaches.
- Good for producing a quick, defensible priority list for small utilities with limited budgets.
- Combine AWWA's prioritized controls with CPG 2.0 checklists for grant applications and board reporting.

21. NERC CIP - Critical Infrastructure Protection Reliability Standards

Issuer / Version: North American Electric Reliability Corporation (NERC); approved and enforced under FERC authority. Standards are CIP-002 through CIP-015; CIP-015 (internal network security monitoring) was approved in 2025.

What it is: Mandatory, auditable cybersecurity standards for the Bulk Electric System (BES) in North America.

Who uses it: Registered entities: generation owners and operators, transmission owners and operators, balancing authorities, and reliability coordinators.

Key contents:

- **CIP-002:** BES Cyber System categorization (High, Medium, Low impact).
- **CIP-003:** security management controls (including Low impact requirements).
- **CIP-004:** personnel and training.
- **CIP-005:** electronic security perimeters and interactive remote access.
- **CIP-006:** physical security of BES Cyber Systems.
- **CIP-007:** system security management (ports and services, patching, malware, logging, accounts).
- **CIP-008:** incident reporting and response planning.
- **CIP-009:** recovery plans.
- **CIP-010:** configuration change management and vulnerability assessments.
- **CIP-011:** information protection.
- **CIP-012:** communications between control centers.
- **CIP-013:** supply chain risk management.
- **CIP-014:** physical security of critical substations.
- **CIP-015:** internal network security monitoring.

How it fits: The most mature mandatory OT security regime in the U.S. Often borrowed as a model by other sectors.

Practical notes:

- Significant per-violation, per-day penalties; audits are evidence-heavy.
- Relevant to water utilities that own generation assets or that interconnect with electric utilities. Also useful as a benchmark for what "regulated OT security" looks like if water regulation expands.
- CIP-005 and CIP-013 are strong templates for remote access and vendor requirements in any OT sector.

22. TSA Security Directives - Pipelines and Rail

Issuer / Version: Transportation Security Administration. Pipeline Security Directive series issued after the 2021 Colonial Pipeline incident, with reissued and revised versions since. Rail directives followed in 2022. A 2024 proposed rule seeks to codify these requirements into regulation.

What it is: Mandatory cybersecurity requirements for designated critical pipeline and rail owners and operators.

Who uses it: TSA-designated hazardous liquid and natural gas pipeline operators, and passenger and freight rail carriers.

Key contents:

- Designate a cybersecurity coordinator available 24/7.
- Report cybersecurity incidents to CISA within tight timeframes.
- Conduct vulnerability assessments.
- **Performance-based requirements** via a TSA-approved Cybersecurity Implementation Plan:
  - network segmentation between IT and OT
  - access control measures
  - continuous monitoring and detection
  - patching of critical systems, or compensating controls
- Maintain and test a Cybersecurity Incident Response Plan.
- Establish a Cybersecurity Assessment Program with annual reporting.

How it fits: Shifted from prescriptive to performance-based in later revisions after industry feedback. Aligns with CSF and CPG concepts.

Practical notes:

- A useful precedent showing how quickly federal OT regulation can arrive after a major incident.
- The Implementation Plan structure (outcome, measure, evidence) is a good model for any OT security plan.

PART 3 - REGULATORY AND CONTRACTUAL REGIMES

23. CMMC 2.0 and DFARS 252.204-7012 (Defense Industrial Base)

Issuer / Version: Department of Defense (now styled Department of War).

- CMMC program rule 32 CFR Part 170, effective December 16, 2024.
- Acquisition rule DFARS 252.204-7021, effective November 10, 2025, which started **Phase 1**.

What it is: A certification program verifying that defense contractors protect Federal Contract Information (FCI) and CUI.

Who uses it: Defense contractors and subcontractors at all tiers handling FCI or CUI.

Key contents:

- **Level 1:** FCI only; 15 basic safeguarding requirements (FAR 52.204-21); annual self-assessment.
- **Level 2:** CUI; 110 requirements of NIST SP 800-171 Rev 2; self-assessment or third-party (C3PAO) assessment every three years, plus annual affirmations.
- **Level 3:** higher-risk CUI; selected SP 800-172 enhanced requirements; government-led (DIBCAC) assessment.
- Limited POA&M allowances ("conditional" status with 180 days to close).
- **DFARS 252.204-7012 (still in force):** implement 800-171; report cyber incidents to DoD within **72 hours**; preserve images; flow down to subcontractors. SPRS score submission under DFARS 7019/7020.

Current status (important):

- On **July 13, 2026**, DoD suspended the transition to **Phase 2** (mandatory C3PAO certification originally set for November 10, 2026) and later phases.
- DoD launched a CMMC Reform Task Force review.
- A class deviation of **September 3, 2026** made the suspension binding on contracting officers.
- Phase 1 self-assessments, SPRS scores, affirmations, and DFARS 7012 **remain in effect**. No replacement Phase 2 date has been published as of this writing.

Practical notes:

- The pause is not a reprieve on security. Remediation for Level 2 is unchanged, and C3PAO backlogs are long.
- Check each contract's actual clause requirements rather than the program timeline.

24. FedRAMP - Federal Risk and Authorization Management Program

Issuer / Version: GSA program office under OMB policy; codified by the FedRAMP Authorization Act (December 2022). Uses NIST SP 800-53 Rev 5 baselines. A modernization initiative, **FedRAMP 20x**, launched in 2025 to automate and accelerate authorizations.

What it is: The standardized government-wide approach to security assessment and authorization for cloud products and services used by federal agencies. The principle is "do once, use many."

Who uses it: Cloud service providers (IaaS, PaaS, SaaS) selling to federal agencies, and agencies consuming cloud services. Many state and local governments use it as a proxy (and StateRAMP builds on it).

Key contents:

- **Impact baselines** tailored from 800-53: Low, LI-SaaS (Tailored Low), Moderate (most common), and High.
- Independent assessment by accredited **Third Party Assessment Organizations (3PAOs)**.
- Authorization packages: SSP, SAR, and POA&M, plus continuous monitoring deliverables (monthly scans, POA&M updates, annual assessments).
- **Authorization paths:** agency authorization, historically the Joint Authorization Board (replaced by the FedRAMP Board structure), and new 20x approaches emphasizing automated, machine-readable evidence (OSCAL) and key security indicators.
- A marketplace listing authorized services.

How it fits: Applies the RMF and 800-53 to the cloud. Relevant to CMMC because cloud services storing CUI must meet FedRAMP Moderate or equivalent.

Practical notes:

- When clients adopt cloud services (including SSO, MFA, and SCADA cloud historians), a FedRAMP authorization is useful due-diligence evidence even for non-federal buyers.
- Check the marketplace for current authorization status and impact level; "in process" is not "authorized."

25. HIPAA Security Rule

Issuer / Version: HHS Office for Civil Rights; 45 CFR Part 164, Subpart C (in effect since 2005). An NPRM with a major overhaul was published in January 2025; confirm whether it has been finalized before citing new requirements. NIST SP 800-66 Rev 2 (February 2024) is the implementation guide.

What it is: A federal regulation requiring safeguards for electronic protected health information (ePHI).

Who uses it: Covered entities (health plans, clearinghouses, most providers) and business associates, including IT and security vendors with ePHI access.

Key contents (current rule):

- **Administrative safeguards:** risk analysis and risk management (the most-cited enforcement failure), security officer, workforce training, contingency planning, and business associate agreements.
- **Physical safeguards:** facility access, workstation and device controls.
- **Technical safeguards:** access control, audit controls, integrity, authentication, and transmission security.
- Specifications are **"required" or "addressable."** Addressable means implement it, or document an equivalent alternative or why it isn't reasonable.

Proposed changes (January 2025 NPRM):

- Eliminate the addressable distinction.
- Require MFA and encryption with limited exceptions.
- Require asset inventories and network maps.
- Require vulnerability scanning and penetration testing.
- Require the ability to restore systems within 72 hours.
- Require annual compliance audits.

How it fits: Risk analysis methodology commonly follows SP 800-30. SP 800-66 maps HIPAA to CSF and 800-53. Breach notification is a separate rule.

Practical notes:

- Water utilities rarely touch HIPAA, except through self-insured employee health plans, which are covered entities.
- Enforcement actions overwhelmingly cite missing or inadequate enterprise-wide risk analysis.

26. SEC Cybersecurity Risk Management and Incident Disclosure Rules

Issuer / Version: U.S. Securities and Exchange Commission; adopted July 2023, effective December 2023.

What it is: Disclosure requirements for public companies on material cybersecurity incidents and on cybersecurity risk management, strategy, and governance.

Who uses it: SEC registrants (public companies), including foreign private issuers via Forms 6-K and 20-F. It also indirectly affects their vendors and service providers.

Key contents:

- **Form 8-K Item 1.05:** disclose a material cybersecurity incident within **four business days** of determining it is material (the determination must be made without unreasonable delay). A limited national security or public safety delay is available through the U.S. Attorney General.
- **Regulation S-K Item 106 (annual 10-K):**
  - Describe processes for assessing, identifying, and managing material cyber risks, including use of third parties.
  - Describe whether cyber risks have materially affected the business.
  - Describe board oversight and management's role and expertise.
- Disclosures must be tagged in Inline XBRL.

How it fits: Pushes cybersecurity into enterprise governance, which CSF 2.0's Govern function supports. Materiality processes should be wired into IR plans alongside CIRCIA and other timelines.

Practical notes:

- Not directly applicable to municipal utilities, but relevant for investor-owned utilities and any public company clients.
- The key operational need is a documented **materiality determination process**, with defined roles among the CISO, legal, the CFO, and the disclosure committee.

27. Federal Cybersecurity Executive Orders and OMB Memoranda (Policy Drivers)

Issuer / Version: The White House and OMB. Key instruments:

- **EO 14028** (May 2021), Improving the Nation's Cybersecurity.
- **EO 14144** (January 2025), later amended by **EO 14306** (June 2025).
- OMB M-22-09 (zero trust), M-21-31 (logging), M-22-18 and M-23-16 (secure software attestation).
- CISA Binding Operational Directives, such as BOD 22-01 (KEV remediation).

What it is: The policy layer that directs federal agencies and shapes requirements that flow down to vendors, and often into private-sector best practice.

Who uses it: Federal agencies (binding); software and cloud suppliers to government (through contracts and attestations); and everyone else as de facto direction on where standards are heading.

Key contents:

- **EO 14028** launched the modern federal push on:
  - zero trust adoption
  - MFA and encryption
  - secure software development (which produced the SSDF attestation)
  - SBOMs
  - standardized incident response playbooks
  - logging requirements
- **EO 14144 / EO 14306** refined priorities on software supply chain security and secure software updates (which drove SP 800-53 Release 5.2.0 and the SSDF update), post-quantum cryptography migration, and AI in cyber defense. Some earlier provisions were rescinded or modified.
- **BOD 22-01:** agencies must remediate KEV-listed vulnerabilities within set deadlines.

How it fits: Explains *why* NIST documents change when they do. Executive action is frequently the trigger for NIST revisions.

Practical notes:

- Policy shifts with administrations. Cite the specific current order and section, and check for amendments or rescissions before relying on it in a deliverable.
- Even non-federal clients benefit from tracking KEV and BOD-driven timelines as a prioritization standard.

PART 4 - KEY NON-GOVERNMENT STANDARDS (FREQUENTLY PAIRED WITH THE ABOVE)

28. ISA/IEC 62443 - Security for Industrial Automation and Control Systems

Issuer / Version: Developed by ISA99 and published jointly by ISA and IEC. A multi-part series, with parts revised on different schedules.

What it is: The leading international consensus standard series for OT and IACS cybersecurity. Unlike NIST guidance, it defines requirements for **asset owners, system integrators, and product suppliers**, and supports formal certification.

Who uses it: Utilities, manufacturers, OT vendors, and integrators. It is increasingly specified in procurement contracts and referenced by governments worldwide.

Structure (four groups):

- **1-x General:** concepts, terminology, and models (zones and conduits, security levels).
- **2-x Policies and procedures:**
  - 2-1: security program requirements for asset owners
  - 2-3: patch management in IACS
  - 2-4: requirements for service providers and integrators
- **3-x System:**
  - 3-2: security risk assessment for system design (zones and conduits)
  - 3-3: system security requirements and security levels
- **4-x Component:**
  - 4-1: secure product development lifecycle for vendors
  - 4-2: technical requirements for components (embedded devices, host devices, network devices, software applications)

Key concepts:

- **Zones and conduits:** group assets by security requirements and control communication between groups.
- **Security Levels SL 1-4:** protection against increasingly capable attackers, from casual violation up to sophisticated, well-resourced actors. There are target (SL-T), capability (SL-C), and achieved (SL-A) variants.
- **Seven Foundational Requirements:**
  - Identification & Authentication Control
  - Use Control
  - System Integrity
  - Data Confidentiality
  - Restricted Data Flow
  - Timely Response to Events
  - Resource Availability

How it fits: SP 800-82 Rev 3 aligns with 62443 concepts; 62443-4-1 parallels SSDF. **ISASecure** provides certification for products and development processes.

Practical notes:

- The 62443-3-2 zones-and-conduits risk assessment is the most practical piece for segmentation projects at treatment plants and lift stations.
- In vendor contracts, require 62443-4-1 and 4-2 certified products, and 62443-2-4 obligations for integrators. This covers remote access, account management, and patch support.
- Parts are paywalled (ISA members get access).

29. ISO/IEC 27001:2022 - Information Security Management Systems (ISMS)

Issuer / Version: ISO and IEC; 2022 edition (Amendment 1 in 2024 added climate change considerations). The transition deadline for 2013-edition certificates was October 31, 2025. Companion guidance is ISO/IEC 27002:2022.

What it is: The international standard for establishing, implementing, maintaining, and continually improving an Information Security Management System. It is **certifiable** by accredited third-party auditors.

Who uses it: Organizations worldwide seeking certifiable assurance, especially vendors and service providers selling internationally or to enterprise customers.

Key contents:

- **Clauses 4-10 (mandatory management system requirements):**
  - context of the organization
  - leadership
  - planning (risk assessment and treatment)
  - support
  - operation
  - performance evaluation (internal audit, management review)
  - improvement
- **Annex A: 93 controls in four themes:** Organizational (37), People (8), Physical (14), Technological (34).
- **New controls in 2022** include threat intelligence, cloud services security, ICT readiness for business continuity, physical security monitoring, configuration management, information deletion, data masking, data leakage prevention, monitoring activities, web filtering, and secure coding.
- **Statement of Applicability (SoA):** documents which controls apply and why.
- **Certification cycle:** initial two-stage audit, annual surveillance audits, and recertification every three years.

How it fits: A management-system wrapper around controls. Maps readily to CSF 2.0 and 800-53. The ISO/IEC 27019 extension covers the energy utility process-control domain.

Practical notes:

- US public utilities rarely pursue certification. It matters most for evaluating vendors (SaaS, managed service providers).
- A SOC 2 report or ISO 27001 certificate is a common vendor due-diligence request; check the scope statement, not just the logo.

30. CIS Critical Security Controls v8.1

Issuer / Version: Center for Internet Security (nonprofit); Version 8.1 (June 2024). Separate from the CIS Benchmarks, which are hardening configuration guides for specific products.

What it is: A prioritized, prescriptive set of defensive actions derived from real-world attack data. It is the most "do this next" of the major frameworks.

Who uses it: Organizations of all sizes, especially small and mid-sized ones and state and local governments (MS-ISAC members). Referenced in some state laws as a reasonable-security benchmark.

Key contents:

- **18 Controls:**
  - Inventory of Enterprise Assets
  - Inventory of Software Assets
  - Data Protection
  - Secure Configuration
  - Account Management
  - Access Control Management
  - Continuous Vulnerability Management
  - Audit Log Management
  - Email & Web Browser Protections
  - Malware Defenses
  - Data Recovery
  - Network Infrastructure Management
  - Network Monitoring & Defense
  - Security Awareness Training
  - Service Provider Management
  - Application Software Security
  - Incident Response Management
  - Penetration Testing
- **153 Safeguards**, sorted into **Implementation Groups:**
  - **IG1:** essential cyber hygiene (56 safeguards); the minimum for every organization.
  - **IG2:** adds safeguards for organizations with more complex environments and sensitive data.
  - **IG3:** full set for organizations facing sophisticated attackers.
- v8.1 added a **Govern** function tag to align with CSF 2.0 and refined asset classes and definitions.
- Free companion tools include the CIS Controls Self Assessment Tool (CSAT) and mappings to CSF, 800-53, ISO, and others.

How it fits: Implementation-level detail under CSF. IG1 overlaps heavily with CPGs 2.0.

Practical notes:

- IG1 is an excellent 90-day remediation plan for small utilities' **IT** side.
- CIS Controls are IT-centric; for SCADA and OT, supplement with SP 800-82, 62443, and CPGs' OT-specific goals.
- MS-ISAC resources (some free) are available to state, local, tribal, and territorial governments, including public utilities.

Suggested Framework Stack for Water/Wastewater OT Engagements

Need	Use
Legal obligation (drinking water)	AWIA §1433 RRA and ERP
Program structure and board reporting	NIST CSF 2.0
First assessment / baseline	CISA CPGs 2.0 (+ AWWA Tool)
Maturity roadmap	DOE C2M2
OT technical depth	NIST SP 800-82 Rev 3
Segmentation design and vendor requirements	ISA/IEC 62443 (3-2, 2-4, 4-1/4-2)
Control catalog when needed	NIST SP 800-53 (OT overlay)
IT hygiene quick wins	CIS Controls IG1
Incident response and reporting	SP 800-61 Rev 3 + CIRCIA readiness
Vendor and supply chain	SP 800-161 Rev 1 + 62443-2-4
Identity and remote access	SP 800-63-4 + zero trust principles

Sources: NIST CSRC, CISA, EPA, DOE, DoD CIO, and issuing bodies. Items marked as proposed or pending (CIRCIA final rule, CMMC Phase 2, HIPAA Security Rule update, SSDF revision) should be re-verified at time of use.