Cybersecurity Controls & Assessments

Building a Defensible Security Program for Critical Infrastructure

TDW
CYBERSECURITY • IT CONSULTING

The Security – Convenience Balance

Cybersecurity is now a part of our personal and professional lives.

With a few exceptions greater security requires greater time, effort, and awareness.

THE STAKES

“You can’t defend what you don’t understand.”

Critical infrastructure is among the most targeted sectors in cybersecurity. For energy utilities and water systems, a successful attack isn’t measured in data breaches — it’s measured in power outages, treatment failures, and public safety emergencies.

An assessment gives you the one thing every security program requires: an accurate picture of where you stand.

What Is a Cybersecurity Assessment?

A cybersecurity assessment is a structured, independent evaluation of an organization's security posture — examining the people, processes, and technology controls protecting critical systems and data.

Unlike a compliance audit, an assessment is designed to produce an honest picture of real risk — not just a checkbox against a standard.

What Gets Evaluated

- Policies, standards, and documentation
- Technical controls and configurations
- Access management and identity controls
- Incident detection and response capability
- Vendor and supply chain exposure
- OT/ICS and operational technology systems

Assessments are most valuable when conducted independently — free of vendor relationships, implementation bias, or internal blind spots.

Two Types of Assessments

Cybersecurity Assessment

Full-Scope Evaluation

A comprehensive evaluation of current security posture across all applicable systems and controls. Includes technical review, documentation analysis, and stakeholder interviews. Produces a risk-tiered findings register, executive summary, and prioritized remediation roadmap.

Best for: Organizations wanting a complete, independent view of their security posture — before a regulatory review, after an incident, or as a periodic baseline.

Gap Assessment

Framework-Based Analysis

A structured comparison of current controls against a specific framework — NERC CIP, NIST CSF, or CISA guidelines. Produces a scored, control-by-control gap register with maturity ratings and a remediation roadmap with prioritized action items.

Best for: Organizations preparing for regulatory audits, seeking a documented baseline, or evaluating compliance before investing in security improvements.

Common Assessment Frameworks

NERC CIP

North American Electric Reliability Corporation Critical Infrastructure Protection

Required for: Bulk electric system operators, electric cooperatives, transmission owners/operators

Mandatory cybersecurity standards for the bulk electric system — covering asset identification, access controls, configuration management, incident reporting, and recovery planning.

NIST CSF

NIST Cybersecurity Framework

Applicable to: Any organization; widely adopted by critical infrastructure operators

Voluntary risk-based framework organized around five functions: Identify, Protect, Detect, Respond, Recover. Provides a common language for cybersecurity risk management.

CISA

Cybersecurity & Infrastructure Security Agency Guidelines

Applicable to: All critical infrastructure sectors; validated by federal cybersecurity authority

Federal guidance and controls for critical infrastructure protection, including sector-specific guidance for energy, water, and emergency services.

The Assessment Process

1

Scope

Define systems, locations, and frameworks in scope. Identify key stakeholders and documentation requirements.

2

Review

Examine existing policies, standards, configurations, and documentation. Conduct stakeholder interviews.

3

Evaluate

Assess technical and administrative controls against the applicable framework. Identify gaps, vulnerabilities, and exposures.

4

Report

Produce risk-tiered findings register with detailed descriptions, risk ratings, and affected assets.

5

Remediate

Deliver prioritized remediation roadmap with short-, mid-, and long-term action items and effort estimates.

Key Control Domains

Access & Identity

User access controls, authentication, privileged account management.

Network Security

Segmentation, firewalls, monitoring, perimeter controls.

Configuration Management

Baseline configs, change control, hardening standards.

Incident Response

Detection, escalation, response, recovery, and reporting procedures.

Patch & Vulnerability Management

Patch cadence, vulnerability scanning, and remediation tracking.

OT / ICS Security

Control system isolation, SCADA security, IT/OT boundary controls.

Physical Security

Facility access controls, tiered by criticality to operations.

Supply Chain & Vendor Risk

Third-party access, vendor assessments, contract controls.

What You Receive

Executive Summary

A plain-language summary of the engagement, key findings, and top-priority actions — written for leadership and board audiences.

Risk-Tiered Findings Register

Control-by-control findings with risk ratings (Critical / High / Medium / Low), affected assets, and detailed descriptions of each gap.

Remediation Roadmap

Prioritized action items organized by timeframe: short-term (quick wins), mid-term (program improvements), and long-term (strategic investments).

Technical Report

Full documentation of scope, methodology, controls evaluated, and findings — suitable for audit evidence and internal governance.

The Remediation Roadmap

Short-Term
0 – 90 Days

- Remediate critical and high-risk findings
- Patch known exploitable vulnerabilities
- Close unauthorized access paths
- Implement missing basic controls

Mid-Term
90 – 180 Days

- Address medium-risk findings
- Improve monitoring and detection
- Strengthen access and configuration management
- Document updated policies and standards

Long-Term
180+ Days

- Mature the security program
- Implement strategic control improvements
- Conduct follow-up validation assessment
- Establish ongoing assessment cadence

Why Use an Independent Assessor?

Objectivity

An internal team assesses what it built. An independent assessor evaluates what's actually there — without institutional bias or familiarity blindness.

Regulatory Credibility

Third-party assessments carry more weight with regulators, auditors, and boards than self-assessments. An independent report is a defensible artifact.

Specialized Expertise

Effective assessment requires deep familiarity with the frameworks, the threat landscape, and the operational environment being assessed. That expertise is rarely available in-house.

No Vendor Conflict

Unlike assessors tied to technology vendors, an independent consultant has no interest in recommending products or services beyond the scope of the engagement.

TDW

CYBERSECURITY • IT CONSULTING

25 years of hands-on critical infrastructure security experience — energy cooperatives, water utilities, and OT/ICS environments. Not a generalist firm. This is specifically what we do.

- Cybersecurity & gap assessments — NERC CIP, NIST CSF, CISA
- OT/ICS and SCADA security program development
- CISA-validated controls for cloud-based critical infrastructure
- 19-year embedded engagements with energy and water utility clients

tdwco.com