

# NIST SP 800-82 Rev. 3 – Moderate OT Overlay

NIST SP 800-82 Rev. 3 (Moderate OT Overlay) guides securing industrial control and operational technology systems with moderate-impact cybersecurity controls.



## What it is

NIST SP 800-82 Rev. 3 (Moderate OT Overlay) is a cybersecurity framework that provides tailored guidance for securing operational technology (OT) systems in industrial and critical infrastructure environments. The Moderate OT Overlay specifically addresses security and risk management requirements for OT systems operating at a moderate impact level, helping organizations mitigate threats to essential industrial processes.

Developed and published by the National Institute of Standards and Technology (NIST), this framework is widely used by asset owners, operators, and security professionals responsible for OT environments. It extends the security controls from NIST SP 800-53 to address OT-specific risks such as process disruptions, equipment compromise, and unique system architectures found in sectors like energy, manufacturing, and transportation.

## At a glance

|                                                                                       |                                                       |                                                        |
|---------------------------------------------------------------------------------------|-------------------------------------------------------|--------------------------------------------------------|
| <div>PUBLISHER</div> <div>National Institute of Standards and Technology (NIST)</div> | <div>TYPE</div> <div>Guidance</div>                   | <div>VERSION</div> <div>Rev. 3</div>                   |
| <div>EFFECTIVE</div> <div>September 28, 2023</div>                                    | <div>DOMAIN</div> <div>Operational Resilience</div>   | <div>FAMILY</div> <div>NIST Special Publications</div> |
| <div>REGION</div> <div>United States</div>                                            | <div>INDUSTRY</div> <div>Energy &amp; Utilities</div> | <div>ADOPTION MODEL</div> <div>Risk Management</div>   |
| <div>IMPLEMENTATION COMPLEXITY</div> <div>High</div>                                  |                                                       |                                                        |

Source: <https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft>

## Why it matters

- **Strengthen risk management for OT systems** Enable systematic identification, assessment, and mitigation of cybersecurity risks specific to industrial and operational technology environments.
- **Enhance regulatory and standards alignment** Support compliance with industry and government cybersecurity regulations through mapped controls tailored for moderate-impact OT systems.
- **Promote operational continuity** Minimize disruptions to essential industrial processes by reducing the likelihood and impact of cyber incidents affecting OT assets.
- **Improve incident detection and response** Facilitate early identification and effective response to threats with controls designed for the unique architectures of OT systems.

## How SmartSuite supports NIST 800-82 Rev.3 Moderate OT

|                                                                                                                                                                          |                                                                                                                                                         |                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>OT Security Control Overlay Library</b><br>Organize OT-specific controls mapped to the NIST 800-82 low-impact overlay for industrial environments.                    | <b>Asset and System Inventory for OT</b><br>Maintain visibility into industrial devices, controllers, and network infrastructure supporting OT systems. | <b>Vulnerability and Patch Management for OT</b><br>Track vulnerabilities affecting OT devices and coordinate remediation actions across operational teams.                |
| <b>Incident Detection and Response for OT Systems</b><br>Manage workflows for investigating and responding to cybersecurity incidents affecting industrial environments. | <b>OT Vendor and Supply Chain Risk Oversight</b><br>Track vendor security posture and third-party access to operational technology systems.             | <b>OT Control and Operational Security Readiness Reporting</b><br>Provide dashboards showing OT control adoption, system risk posture, and operational security readiness. |

## Common framework mappings

- CIS Controls v8.1
- ISO 27001:2022
- NERC CIP
- NIST CSF 2.0
- NIST 800-53 Rev.5
- PCI DSS 4.0.1
- SOC 2

## Official resources

**NIST SP 800-82 Rev. 3 Guide**  
Defines security measures and controls for protecting Operational Technology environments.  
[csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft](https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft)

## Frequently asked questions

- What is NIST SP 800-82 Rev. 3 (Moderate OT Overlay) used for?**  
NIST SP 800-82 Rev. 3 provides guidelines for securing operational technology (OT), such as industrial control systems (ICS), in alignment with the NIST Cybersecurity Framework. The Moderate OT Overlay tailors baseline security controls for environments requiring a moderate level of security assurance, helping organizations protect critical infrastructure from cyber threats.
- Is compliance with NIST SP 800-82 Rev. 3 mandatory?**  
Compliance with NIST SP 800-82 Rev. 3 is generally not mandatory except for U.S. federal agencies or organizations handling regulated infrastructure. However, applying this framework is considered industry best practice for enhancing OT security and may be required by contractual or sector-specific regulatory obligations.
- What systems or environments does the Moderate OT Overlay apply to?**  
The Moderate OT Overlay is intended for operational technology environments where compromise could have moderate adverse effects on organizational operations, assets, or individuals. This includes systems in sectors such as energy, water, manufacturing, and transportation with moderate confidentiality, integrity, and availability requirements.
- What are key artifacts or control requirements in the Moderate OT Overlay?**  
Key artifacts include the security control baseline tailored for OT assets, risk assessment documentation, asset inventories, and implementation evidence for security controls. Organizations are expected to implement and document controls such as access management, network segmentation, system monitoring, and incident response planning.
- How do organizations implement NIST SP 800-82 Rev. 3 (Moderate OT Overlay)?**  
Implementation starts with identifying OT assets, conducting a risk assessment specific to OT, and applying the recommended moderate baseline controls. Organizations should adapt controls to their environment through a risk-based approach, using the guidance provided to address unique OT system requirements.

### **How does NIST SP 800-82 Rev. 3 relate to other frameworks like NIST SP 800-53 or ISA/IEC 62443?**

NIST SP 800-82 Rev. 3 adapts the control catalog of NIST SP 800-53 specifically for OT environments, providing sector-tailored guidance. It is complementary to other OT security frameworks such as ISA/IEC 62443, allowing organizations to map and align controls for comprehensive coverage.

### **What are the ongoing compliance requirements for the Moderate OT Overlay?**

Ongoing compliance involves regular review and updating of OT asset inventories, periodic risk assessments, continuous monitoring of control effectiveness, incident response exercises, and maintenance of documentation. Reassessment is necessary upon significant system changes or emerging threats.

### **How would SmartSuite support NIST SP 800-82 Rev. 3 (Moderate OT Overlay)?**

SmartSuite helps organizations manage NIST SP 800-82 Rev. 3 by facilitating risk tracking, control management, and evidence collection tailored to OT assets. It supports audit readiness with centralized documentation, automated workflows for control reviews, and robust reporting capabilities for demonstrating ongoing compliance.

License included / downloadable: Yes NIST SP 800-82 Rev. 3 (Moderate OT Overlay) is publicly available for free from NIST's website. License included with platform

Full framework page and mappings: [smartsuite.com/frameworks/nist-sp-800-82-rev-3-moderate-ot-overlay-guide-to-operational-technology-ot-security](https://smartsuite.com/frameworks/nist-sp-800-82-rev-3-moderate-ot-overlay-guide-to-operational-technology-ot-security)