# DATA DIODE FOR CIS CONTROLS COMPLIANCES

## HOW DATA DIODE HELPS AN ORGANIZATION TO COMPLY WITH CIS CONTROLS

CONNEXITE

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

The **CIS Controls for Industrial Control Systems (ICS)** is a globally recognized cybersecurity framework developed by the Center for Internet Security. It provides a prioritized set of defensive actions specifically tailored for operational technology (OT) environments, guiding asset owners in securing critical infrastructure like manufacturing plants, power grids, water treatment facilities, and more. The v8.1 ICS edition maps these actions to the unique risks and constraints of ICS, including real-time system requirements, legacy components, and safety-critical operations.

ICS environments face increasingly frequent and sophisticated cyber threats—from ransomware that halts production to state-sponsored attacks targeting energy systems. The CIS Controls v8.1 provides a practical, tested roadmap for resilience, covering everything from asset inventory and configuration management to secure data flow and audit logging.

**ConnexOne**, our high-assurance, hardware-enforced **unidirectional gateway**, plays a pivotal role in achieving the goals laid out in the CIS Controls v8.1 ICS guide. While many safeguards rely on policies or software enforcement, ConnexOne offers **physically enforced data integrity** by ensuring that **information flows only one way—from ICS to enterprise, never back**. This unidirectional flow is vital in scenarios where confidentiality, system integrity, and availability are non-negotiable.

Some of the key benefits of Connexone and its alignment to CIS Controls are as follows:

**Log and Event Forwarding (Controls 8, 10, 13):**
ConnexOne securely transmits system logs, malware alerts, sensor informations and network telemetry to SIEM or SOC platforms without exposing ICS systems to external threats.

**Data Protection (Control 3):**
It ensures secure and tamper-proof delivery of sensitive data (sensor values, process status, performance indicators) to SCADA, historian, or analytics platforms—supporting encrypted and policy-bound data egress.

**Network Segmentation (Control 12):**
ConnexOne enforces physical segmentation between control and enterprise zones, closing the door to threats like lateral movement or reverse command channels.

**Inventory and Configuration Compliance (Controls 1, 2, 4):**
Asset and software inventory data can be safely exported to IT management systems, enabling centralized visibility without risking attack vectors like remote misconfiguration or update tampering.

**Backup and Recovery Reporting (Control 11):**
ConnexOne can transmit success/failure alerts of backup and recovery processes to administrative systems without granting access to the ICS domain.

**Complementary Support for Business Analytics and SCADA Integration:**
ICS-generated data often powers SCADA dashboards and business intelligence tools. ConnexOne provides a secure conduit to relay this data outward, aligning with the guide's emphasis on controlled data delivery without introducing inbound risk.

So, in conclusion, CIS Controls v8.1 for ICS outlines the cybersecurity essentials for protecting our most critical infrastructure. **ConnexOne** stands as a cornerstone technology for achieving compliance with these controls by providing **uncompromising one-way data transfer**, securing data flow from OT to IT, and ensuring operations remain **resilient, observable, and safe**.

By combining ConnexOne with the CIS framework, organizations gain a robust, standards-aligned approach to **cyber hygiene and proactive defense** in OT environments—without compromising uptime or safety.

# INTRODUCTION

Industrial Control Systems (ICS) are at the heart of national infrastructure and critical industries—power generation, water treatment, oil and gas, manufacturing, and transportation. These environments, traditionally isolated, are increasingly being integrated with enterprise IT systems to improve operational visibility, decision-making, and efficiency. However, this convergence introduces new vulnerabilities that adversaries actively exploit.

To address the rising cyber threats targeting ICS environments, the **Center for Internet Security (CIS)** developed the **CIS Controls v8.1 for ICS**—a specialized framework designed to help asset owners and operators improve their cybersecurity posture using practical, prioritized defensive measures. Unlike traditional IT security frameworks, CIS Controls v8.1 considers the operational constraints of ICS environments, such as legacy systems, real-time requirements, and the need for continuous availability.

As organizations strive to align with this framework, one of the most critical and often overlooked aspects is **how to securely transmit operational data**—such as logs, alarms, and performance metrics—from ICS networks to external platforms like SCADA systems, business analytics dashboards, or cloud-based monitoring tools. Ensuring that this data leaves the ICS without creating a reverse attack path is a non-trivial challenge.

This is where **ConnexOne**, a high-assurance **hardware-enforced unidirectional gateway**, becomes an essential component of a secure ICS architecture. By physically enforcing a one-way data flow, ConnexOne ensures that critical ICS systems can share necessary information with enterprise or cloud systems—**without allowing any data or threat to re-enter the control environment**.

This document explores how ConnexOne directly supports compliance with CIS Controls v8.1 for ICS and enhances the overall security of operational environments. It highlights specific controls where ConnexOne is not only complementary but often necessary to achieve true separation and protection.

## KEY COMPONENTS

The Controls are divided into **18 control categories**, each further subdivided into safeguards (formerly called sub-controls). In the ICS guide, these controls are contextualized for operational technology. The **key components** include:

- **Asset Management (Controls 1 & 2)**
    - Identifying and managing hardware and software across ICS environments.
- **Access Management (Controls 5 & 6)**
    - Controlling user accounts and permissions, including privileged access.
- **Data and Log Protection (Controls 3, 8, 10, 13)**
    - Securing sensitive data in transit, collecting audit logs, and ensuring logs reach SIEMs.
- **Vulnerability and Configuration Management (Controls 4 & 7)**
    - Maintaining secure configurations and patching systems when feasible in ICS environments.
- **Network Segmentation and Defense (Controls 12 & 13)**
    - Implementing physical and logical segmentation to isolate ICS from less trusted networks.
- **Backup and Recovery (Control 11)**
    - Ensuring data can be restored after a disruption without introducing malware.
- **Security Awareness and Governance (Controls 14–18)**
    - Addressing training, policies, incident response, and third-party management.

## USAGE IN INDUSTRY

CIS Controls are widely adopted across sectors that prioritize **practical, baseline cybersecurity**. In ICS environments, they are particularly relevant for:

- **Energy** (power generation, smart grids)
- **Water/Wastewater Utilities**
- **Manufacturing & Industrial Automation**
- **Transportation & Rail Systems**
- **Oil & Gas**
- **Defense Contractors**

These controls are also **aligned with NIST**, **ISA/IEC 62443**, and **NERC CIP**, making them useful in both regulatory and voluntary security frameworks.

## IMPLEMENTATION PROCESS

Implementing CIS Controls in ICS follows a **risk-based, staged approach**, often tailored to constraints such as uptime, legacy systems, and safety requirements.

**Scoping and Assessment**

- Identify which ICS assets and zones are in scope.
- Conduct an initial gap assessment to identify missing controls.

**Prioritization**

- Use the **IG (Implementation Group)** model (IG1, IG2, IG3) to apply controls according to organizational size and risk level.

**Incremental Deployment**

- Start with foundational controls (inventory, logging, network segmentation).
- Integrate protections into existing OT/ICS processes without disrupting operations.

**Technology Integration**

- Incorporate **ConnexOne** or other technologies to enforce physical segmentation and secure data delivery—especially for controls like centralized logging and secure architecture.

**Validation and Monitoring**

- Monitor compliance and effectiveness of controls.
- Regularly update the asset inventory and conduct periodic audits.

**Continuous Improvement**

- Align control implementation with incident learnings, threat intelligence, and evolving risks.

CIS Controls v8.1 for ICS provide a **practical and achievable roadmap** for securing OT environments. With the help of trusted technologies like **ConnexOne**, organizations can not only meet control requirements such as secure data flow, centralized logging, and segmentation—but also raise the overall resilience of their industrial operations.

# DATA DIODE CONCEPTS

Data diodes are devices designed to enforce one-way data transmission, with its hardware design, preventing any reverse flow of information. This unique characteristic makes them highly effective in protecting critical networks from cyber-attacks. Their application is particularly beneficial in environments that require stringent security measures and regulatory compliance.

Data diodes significantly enhance security by creating an impenetrable barrier for cyber threats. Unlike traditional security solutions that rely on software to control data flow, data diodes provide a physical separation that eliminates the risk of unauthorized access from external networks. This hardware-enforced unidirectional flow ensures that sensitive information, such as financial data, transaction records, and personal customer information, cannot be accessed or manipulated by malicious entities. This level of security is crucial for protecting against sophisticated cyber-attacks and ensuring the integrity of critical systems in financial institutions.


Ensuring the integrity of transmitted data is another critical benefit of data diodes. By allowing data to travel in only one direction, data diode devices prevent any potential tampering or corruption during transmission. This is particularly important in the financial sector, where the accuracy and reliability of data are paramount.

Data diodes are hardware-enforced unidirectional gateways that permit data to flow in only one direction. They are crucial in safeguarding Industrial Control Systems (ICS) by preventing cyber threats from infiltrating critical operational networks. This report explores how data diodes can be effectively utilized to comply with specific CIS Controls v8.1, particularly within ICS environments.

Data diodes function as physical barriers that allow data to exit a secure network without permitting any inbound communication. This unidirectional flow is vital for ICS environments where the integrity and availability of operational data are paramount. By ensuring that data can be transmitted outwards for monitoring or analysis without exposing the control systems to external threats, data diodes uphold the security and reliability of critical infrastructure.

# USE OF DATA DIODES FOR CIS CONTROLS COMPLIANCES

The CIS Controls v8.1 provide a comprehensive framework for enhancing cybersecurity across various domains. Data diodes can play a significant role in meeting several of these controls within ICS settings:

**Control 1: Inventory and Control of Enterprise Assets**

**Safeguard 1.4: Maintain Detailed Asset Inventory**

Data diodes can facilitate the secure transmission of asset inventory data from ICS environments to centralized management systems. This ensures that asset inventories are up-to-date without exposing the ICS to potential threats from bidirectional communication channels.

**Control 2: Inventory and Control of Software Assets**

**Safeguard 2.3: Address Unauthorized Software**

By using data diodes to transmit software inventory logs to centralized systems, organizations can detect and address unauthorized software installations in ICS environments without risking inbound threats.

**Control 3: Data Protection**

**Safeguard 3.4: Encrypt Sensitive Data in Transit**

Data diodes inherently enforce unidirectional data flow, which complements encryption efforts by ensuring that sensitive data transmitted from ICS to external networks cannot be intercepted or altered by malicious actors.

**Control 4: Secure Configuration of Enterprise Assets and Software**

**Safeguard 4.6: Securely Manage Enterprise Assets and Software Configuration**

Data diodes can enforce unidirectional data flows, ensuring that configuration changes or updates to ICS assets originate from a secure, controlled environment. This prevents unauthorized or unintended configuration changes from external networks, maintaining the integrity of critical systems.

**Control 5: Account Management**

**Safeguard 5.1: Establish and Maintain an Inventory of Accounts**

Data diodes can securely transmit account logs from ICS to centralized identity management systems, aiding in the maintenance of accurate account inventories and detection of unauthorized accounts.

**Control 6: Access Control Management**

**Safeguard 6.3: Require MFA for Remote Network Access**

While data diodes enforce unidirectional data flow, they can complement access control measures by ensuring that authentication logs are securely transmitted to monitoring systems, aiding in the enforcement of multi-factor authentication policies.

**Control 7: Continuous Vulnerability Management**

**Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**

By using data diodes to transmit vulnerability scan results from ICS environments to centralized management systems, organizations can continuously monitor and address vulnerabilities without exposing the ICS to potential threats from bidirectional communication channels.

**Control 8: Audit Log Management**

**Safeguard 8.1: Collect Audit Logs**

Implementing data diodes allows for the secure transmission of audit logs from ICS to centralized logging systems, ensuring that logs are collected without exposing the ICS to potential threats.

**Control 9: Email and Web Browser Protections**

**Safeguard 9.2: Use DNS Filtering Services**

Data diodes can help in transmitting DNS query logs to centralized systems for analysis, aiding in the detection and prevention of malicious domains without allowing inbound connections.

**Control 10: Malware Defenses**

**Safeguard 10.4: Centralize Anti-Malware Logging**

Implementing data diodes allows for the secure transmission of anti-malware logs from ICS to centralized logging systems. This ensures that malware detection activities are monitored without risking the introduction of malware through inbound connections.

**Control 11: Data Recovery**

**Safeguard 11.1: Establish and Maintain a Data Recovery Process**

By using data diodes to transmit backup logs and recovery status reports to centralized systems, organizations can monitor data recovery processes in ICS environments without risking inbound threats.

**Control 12: Network Infrastructure Management**

**Safeguard 12.1: Establish and Maintain a Secure Network Architecture**

Data diodes contribute to a secure network architecture by physically enforcing unidirectional data flows, effectively segmenting networks and preventing unauthorized access or data exfiltration from critical ICS components.

**Control 13: Network Monitoring and Defense**

**Safeguard 13.1: Centralize Security Event Alerting**

By using data diodes to transmit logs and alerts from ICS to centralized Security Information and Event Management (SIEM) systems, organizations can monitor security events without risking inbound threats to the control systems.

**Control 14: Security Awareness and Skills Training**

**Safeguard 14.2: Train Workforce on Recognizing Social Engineering Attacks**

While not directly related to data diodes, ensuring that personnel understand the limitations and purposes of unidirectional gateways can enhance overall security awareness and prevent attempts to bypass such controls.

**Control 15: Service Provider Management**

**Safeguard 15.3: Require Security Controls for Service Providers**

When engaging with service providers, data diodes can be used to ensure that data shared from ICS environments is transmitted securely and unidirectionally, mitigating the risk of external threats infiltrating through third-party connections.

**Control 16: Application Software Security**

**Safeguard 16.4: Establish and Maintain a Secure Application Development Process**

Data diodes can facilitate the secure transmission of application development logs and security test results from ICS environments to centralized development teams, ensuring that application security is maintained without exposing the ICS to potential threats.

Incorporating data diodes into ICS environments is a robust strategy for enhancing cybersecurity and ensuring compliance with CIS Controls v8.1. By enforcing unidirectional data flow, organizations can protect critical control systems from external threats while maintaining necessary data transmissions for monitoring and analysis. This approach not only aligns with best practices outlined in the CIS Controls but also fortifies the resilience of essential infrastructure against evolving cyber threats.

## CIS CONTROLS - CONNEXONE USAGE MATRIX

| CIS Control / Safeguard | Relevance | How ConnexONE Supports It |
|---|---|---|
| **Control 13.1**<br>**Centralize Security Event Alerting** | 1 - Inevitable | Secure log streaming from ICS to SIEM without return path |
| **Control 8.1**<br>**Collect Audit Logs** | 1 - Inevitable | Enforces unidirectional flow of sensitive ICS logs to log server |
| **Control 10.4**<br>**Centralize Anti-Malware Logging** | 1 - Inevitable | Malware logs from ICS can be sent securely outward |
| **Control 3.4**<br>**Encrypt Sensitive Data in Transit** | 1 - Inevitable | Data diode ensures integrity even without active encryption enforcement |
| **Control 7.1**<br>**Maintain Vulnerability Management Process** | 2 - Enhancing | Allows scan results and patch states to be monitored externally |
| **Control 4.6**<br>**Securely Manage Enterprise Assets and Software Configuration** | 2 - Enhancing | Prevents unauthorized inbound changes; configurations exported securely |
| **Control 12.1**<br>**Maintain a Secure Network Architecture** | 2 - Enhancing | Enforces physical network segmentation and segmentation policy by design |
| **Control 1.4**<br>**Maintain Detailed Asset Inventory** | 2 - Enhancing | Ensures asset data can leave ICS zone for monitoring without exposure |
| **Control 2.3**<br>**Address Unauthorized Software** | 2 - Enhancing | Transmit unauthorized software detection logs safely to admin systems |
| **Control 5.1**<br>**Maintain Inventory of Accounts** | 2 - Enhancing | Account usage records sent safely for analysis |
| **Control 15.3**<br>**Require Security Controls for Service Providers** | 2 - Enhancing | Limits data exposure to service providers; only outbound diagnostics allowed |
| **Control 11.1**<br>**Establish a Data Recovery Process** | 3 - Optional | Backup logs or success/failure notifications can be sent out via diode |
| **Control 6.3**<br>**Require MFA for Remote Access** | 3 - Optional | Diode can log and send auth events but doesn't directly enforce MFA |
| **Control 9.2**<br>**Use DNS Filtering Services** | 3 - Optional | DNS telemetry data can be sent to external analyzers securely |
| **Control 16.4**<br>**Maintain a Secure Application Development Process** | 3 - Optional | Development logs or deployment checks can be offloaded outward securely |

| | | |
|---|---|---|
| **Control 14.2**<br>**Train Workforce on Social Engineering Awareness** | 3 - Optional | Diodes do not directly help here, but usage education improves awareness |

# ADVANTAGES OF DATA DIODES

Data diodes offer several advantages over traditional security measures:

**Absolute Unidirectional Flow**: Unlike software-based solutions, data diodes physically enforce one-way data transmission, eliminating the risk of reverse flow.

**Robust Security**: Provide a higher level of security by preventing data breaches and unauthorized access.

**Regulatory Compliance**: Support adherence to stringent data protection laws, helping institutions avoid penalties.

**Cost-Effective**: Reduce the need for complex security software and lower overall security costs.

Below table provide a quick comparison between data diode and software-based solutions

| *FEATURE* | DATA DIODE | SOFTWARE SOLUTIONS |
|---|---|---|
| ***Data Flow Control*** | *One-Way (Unidirectional)* | *Two-Way (Bidirectional)* |
| ***Security Level*** | *Strict* | *High* |
| ***Risk of reverse flow*** | *None* | *Always* |
| ***Maintenance Requirements*** | *Low* | *High* |
| ***Regulatory Compliance*** | *Strong/Mandatory* | *Strong/Mandatory* |

A quick comparison of data diode with other solutions

# CONCLUSION

As industrial environments face escalating cyber threats, the **CIS Controls v8.1 for ICS** offer a timely and structured framework to help organizations prioritize their cybersecurity investments and reduce operational risk. These controls are uniquely tailored to address the realities of operational technology—balancing security with the need for availability, safety, and legacy system support. From asset visibility to network segmentation, the Controls provide a roadmap for both foundational hygiene and advanced defensive strategies.

**ConnexOne** emerges as a critical enabler for many of the controls outlined in the guide. By enforcing **hardware-level unidirectional data flow**, ConnexOne ensures that sensitive data such as logs, telemetry, or business analytics can be securely transmitted from ICS environments to enterprise systems—**without any risk of external intrusion or reverse channel exploitation**. This is especially vital for controls requiring centralized monitoring, audit log collection, and network architecture hardening. ConnexOne not only supports compliance but adds a layer of physical assurance unmatched by software-based firewalls or policies.

Ultimately, achieving robust ICS cybersecurity requires both **strategic guidance and tactical enforcement**. The CIS Controls v8.1 provide the strategy; ConnexOne delivers the enforcement. Together, they enable industrial operators to meet regulatory expectations, align with global best practices, and—most importantly—ensure safe, secure, and resilient operations in an increasingly interconnected world.