The SCADAfence Governance Portal
ISO 27001 Cyber Security Framework Compliance

Technical Whitepaper

SCADAfence ISO-27001 Compliance

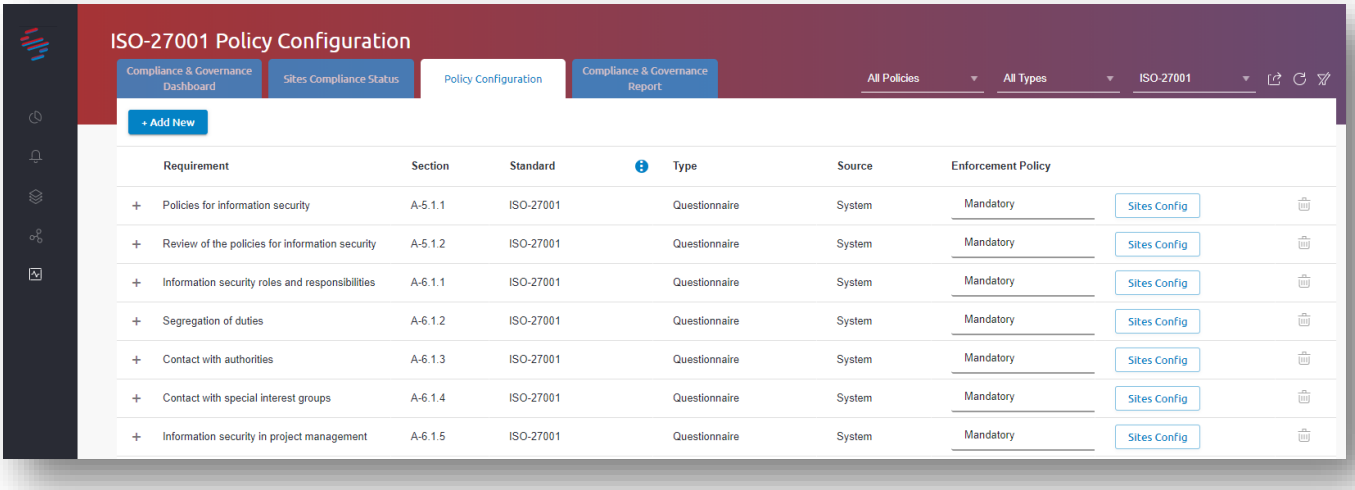
The SCADAfence Platform for OT cyber security, combined with SCADAfence's unique Governance Portal, help utility companies ensure that they meet all controls specified in ISO-27001's compliance requitements.

ISO/IEC 27001 is the leading international standard focused on information security, published by the International Organization for Standardization (ISO), in partnership with the International Electrotechnical Commission (IEC). Both are leading international organizations that develop international standards.
ISO-27001 is part of a set of standards developed to handle information security: the ISO/IEC 27000 series.

The SCADAfence Governance Portal includes a built-in ISO-27001 module which provides cross-organizational tracking and measurement of ISO-27001 adherence.

The SCADAfence Governance Portal provides:

- Fully automated compliance dashboards and detailed compliance reports.
- Compliance status trends and comparison over time.
- Accurate and up-to-date compliance status based on real network traffic data analytics.
- Tracking and measurement of regulations and organizational best practices which are solely based on questionnaires & documentation by using the Manual Questionnaire feature.



 ©Confidential and Proprietary Information of SCADAfence Ltd.

SCADAfence

The SCADAfence Governance Portal
ISO 27001 Cyber Security Framework Compliance

Technical Whitepaper

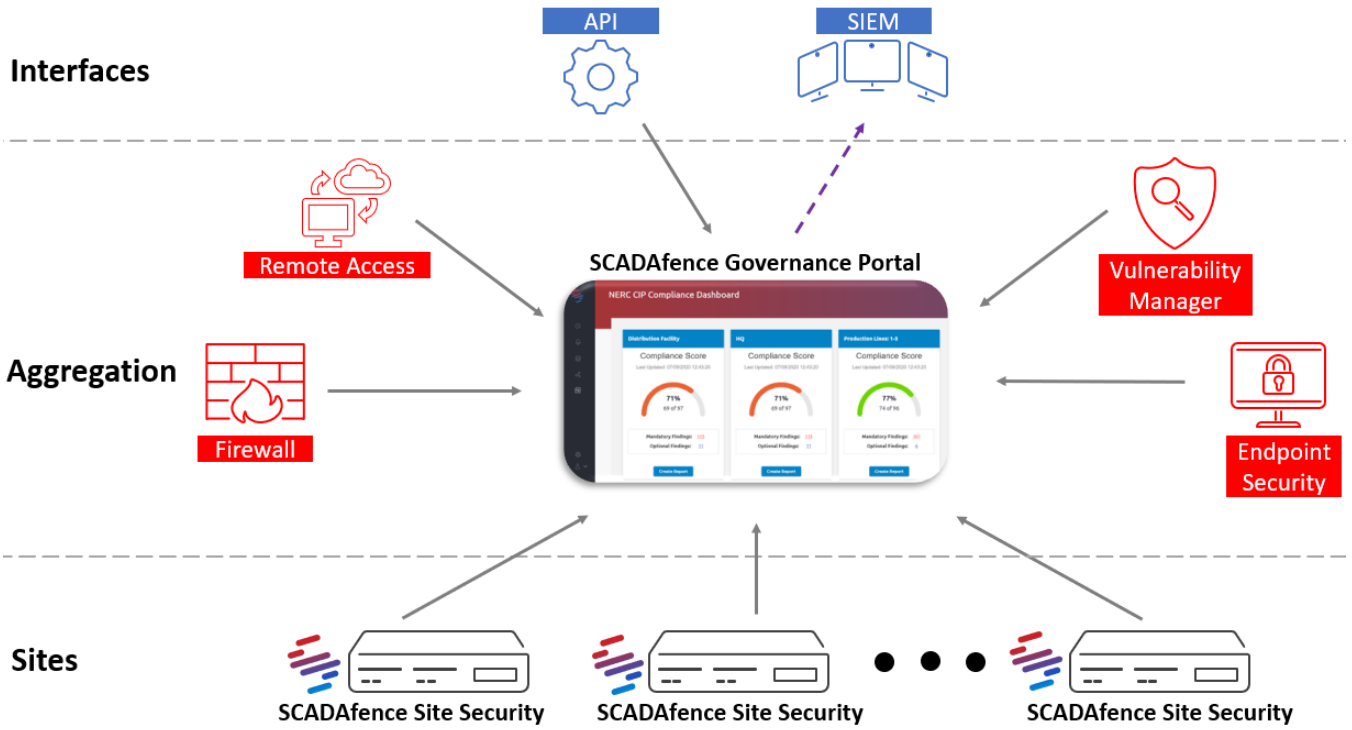
Organizational-Wide Compliance Management

The SCADAfence Governance Portal allows easy and simple integration with 3rd party security and orchestration controls (Firewalls, Endpoint Security, ticketing systems, etc.).

This provides the following advantages:

- **Maximum coverage** – addressing all types of requirements
- **Single pane of glass** - monitor compliance from a central system

The generic integration mechanism opens SCADAfence's Governance Portal to any external source for enhanced compliance coverage and measurement based on accurate external inputs.



 ©Confidential and Proprietary Information of SCADAfence Ltd.

SCADAfence

The SCADAfence Governance Portal
ISO 27001 Cyber Security Framework Compliance

Technical Whitepaper

How SCADAfence Supports ISO-27001 Controls

A.5.1 - Information Security Policy:

To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

The SCADAfence Governance Portal:

Provides full management of your compliance status in a central place. The SCADAfence Governance Portal allows users to attach risk and compliance evidence for continuous monitoring of the security level which can be shared with all relevant stakeholders at any given time by automatically generating a compliance report.

A.6.1 - Internal Organization:

To manage information security within the organization.

The SCADAfence Multi Site Portal & the SCADAfence Platform:

Provide real time information about the security status of the organization. The security status is based on real time data (network traffic monitoring) which generates accurate security alerts which can easily be sent to SIEM and SOC applications as well as shared via email with the relevant owners.

The SCADAfence Multi Site Portal enables users to monitor the current status of their entire organization from a central location by collecting information from different sites and physical locations.

©Confidential and Proprietary Information of SCADAfence Ltd.

SCADAfence

The SCADAfence Governance Portal
ISO 27001 Cyber Security Framework Compliance

A.6.2 - External Parties:

To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

The SCADAfence Platform:

Automatically generates real time alerts on unauthorized remote connections and detects potential vulnerabilities (such as insecure protocols) that might expose the organization to risks from external parties.

In addition, SCADAfence offers an advanced remote OT security solution that correlates between user activities and logged-in accounts. This provides visibility to external communication and allows tracking of the entire chain of events up to the actual industrial commands within the OT network.

A.7.1 - Responsibility for Assets:

To achieve and maintain appropriate protection of organizational assets.

The SCADAfence Platform:

Automatically discovers and creates an accurate asset list of all ICS devices.

The asset inventory provides an up-to-date inventory of devices such as: engineering workstations, HMIs, PLCs, RTUs and I/Os.

Users can also manually add important information for easier and more effective management of their asset inventory.

 ©Confidential and Proprietary Information of SCADAfence Ltd.

SCADAfence

The SCADAfence Governance Portal
ISO 27001 Cyber Security Framework Compliance

Technical Whitepaper

A.7.2 - Information Classification:

To ensure that information receives an appropriate level of protection.

The SCADAfence Platform:

Leverages its deep packet inspection capabilities in order to extract asset related information and automatically categorize assets by different attributes such as: OS, vendor, device type, etc.

In addition, the SCADAfence Platform includes a Threat Assessment module which allows users to prioritize assets by their criticality and risk exposure level to ensure the appropriate protection is in place.

A.10.1 - Operational Procedures and Responsibilities:

To ensure the correct and secure operation of information processing facilities.

The SCADAfence Platform:

Configuration and programming changes performed on ICS devices are automatically monitored and logged by the SCADAfence Platform which generates real-time alerts.

The detailed and comprehensive information collected by the SCADAfence Platform enables users to validate the integrity of the ICS devices and their software which are not secure by nature.

A.10.3 - System Planning and Acceptance:

To minimize the risk of systems failures.

The SCADAfence Platform:

Provides alerts and indications that industrial processes and systems are compromised and might fail to operate.

Security indications such as malware detection as well as operational indications such as machine malfunction or network latency are triggered in real time and allows the organization to respond in a timely manner.

©Confidential and Proprietary Information of SCADAfence Ltd.

SCADAfence

The SCADAfence Governance Portal
ISO 27001 Cyber Security Framework Compliance

Technical Whitepaper

A.10.4 - Protection Against Malicious and Mobile Code:

To protect the integrity of software and information.

The SCADAfence Platform:

Automatically detects A wide variety of malwares and exploits.

Real-time alerts on such malicious tools and attacks helps in responding quickly and effectively to such threats.

In addition, the SCADAfence Platform alerts on the use of insecure protocols which allows users to mitigate the risk of exposure to malicious activity before it becomes an actual threat.

A.10.6 - Network Security Management:

To ensure the protection of information in networks and the protection of the supporting infrastructure.

The SCADAfence Platform:

Provides visibility and enforcement capabilities for network segmentation.

The built-in Network map visualizes the entire network flows including all devices.

The Exposure Analyzer provides the ability to define logical groups and segments for specific tracking and monitoring of communication.

The Exposure Analyzer also provides the ability to define rules which alert in real-time on unauthorized communication between segments.

This allows to inspect communication between control segments, the DMZ and external networks, and detect site-to-site and site-to-corporate network connections.

Once an alert is triggered, automatic enforcement actions can take place using integration with 3rd party applications such as Firewalls and NACs to block traffic.

The SCADAfence Platform will alert on any new communication from the control segment to an external network and vice-versa.

©Confidential and Proprietary Information of SCADAfence Ltd.

SCADAfence

The SCADAfence Governance Portal
ISO 27001 Cyber Security Framework Compliance

Technical Whitepaper

A.10.10 - Monitoring:

To detect unauthorized information processing activities.

The SCADAfence Platform:

Performs continuous network traffic monitoring and provides real-time accurate alerts based on profound domain-expertise and understanding of the ICS field.

SCADAfence leverages its granular anomaly detection mechanism to identify and alert on exposure to various threats and security risks.

Threats and risks include insecure methods of communication, network scanning attempts, data breaches, malwares & exploits as well as ICS device tampering.

Detected threats result in real-time alerts which are automatically prioritized and categorized to ensure easy and quick response by severity.

A.11.2 - User Access Management:

To ensure authorized user access and to prevent unauthorized access to information systems.

The SCADAfence Platform:

Provides network access and authentication continuous monitoring for both OT & IT protocols such as HTTP, HTTPS, FTP, SFTP, SMB and Telnet.

The SCADAfence Platform alerts in real-time on excessive failed login attempts, brute-force attempts and in cases where authentication is performed using unsecure methods and protocols (e.g. the usage of default credentials or insecure protocols).

©Confidential and Proprietary Information of SCADAfence Ltd.

SCADAfence

The SCADAfence Governance Portal
ISO 27001 Cyber Security Framework Compliance

Technical Whitepaper

A.11.3 - User Responsibilities:

To prevent unauthorized user access, and compromise or theft of information and information processing facilities.

The SCADAfence Platform:

Serves as a compensating control and alerts in real-time in case the use of insecure methods such as plain-text protocols, default & weak passwords and insecure protocols.

This real-time detection helps users to easily address these cases and effectively enforce the identification and authentication requirement.

A.12.1 - Security Requirements of Information Systems:

To ensure that security is an integral part of information systems.

The SCADAfence Platform:

Provides a holistic security solution and an accurate up-to-date view of the current security status throughout the network.

The SCADAfence Platform's ability to detect vulnerabilities, malware & exploits as well as monitor the entire network traffic helps users to ensure that other security controls such as Antivirus applications, Firewalls and NACs are configured properly and serve their purpose in securing the estate.

A.12.3 - Cryptographic Controls:

To protect the confidentiality, authenticity or integrity of information by cryptographic means.

The SCADAfence Platform:

The use of insecure and plain-text protocols highly increases the risk of attackers taking advantage of exploits to infect the network with malicious code or gain access to sensitive information.

The SCADAfence Platform provides various controls to identify known exploits and vulnerabilities and also provides alerts in real-time when communication is done using insecure manners (e.g. obsolete protocols, plain-text protocols, etc.)

©Confidential and Proprietary Information of SCADAfence Ltd.

SCADAfence

The SCADAfence Governance Portal
ISO 27001 Cyber Security Framework Compliance

Technical Whitepaper

A.12.6 - Technical Vulnerability Management:

To reduce risks resulting from exploitation of published technical vulnerabilities.

The SCADAfence Platform:

Automatically alerts in real-time on vulnerabilities, malwares & exploits as well as on ICS device configuration changes which exposes assets to threats. In addition, the SCADAfence Platform provides a CVE management module with detailed information about the CVE and affected ICS assets.

A.13.1 - Reporting Information Security Events and Weaknesses:

To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

The SCADAfence Platform:

The SCADAfence Platform's centric workflow UI provides various capabilities that ensure the ease of incidents management and investigation.

The SCADAfence Platform provides all necessary information for an effective investigation and allows users to distribute alerts for investigation via syslog or email, add user comments to each alert and resolve them once investigation is complete.

The SCADAfence Platform supports integration with SIEM and SOC applications for simple collaboration and easy response.

©Confidential and Proprietary Information of SCADAfence Ltd.

SCADAfence

The SCADAfence Governance Portal
ISO 27001 Cyber Security Framework Compliance

Technical Whitepaper

A.15 - Compliance:

- Compliance with legal requirements.
- Compliance with security policies and standards, and technical compliance.
- Information systems audit considerations.

The SCADAfence Governance Portal:

The SCADAfence Governance module offers the ability to define compliance enforcement policies and continuously monitor compliance enforcement status for various ICS standards, frameworks and regulations. It measures compliance progress made over time across all sites and identifies all of the gaps and bottlenecks.

The SCADAfence Governance Portal supports top industry standards and regulations such as:

ISO-27001

IEC-62443

NIST CSF

NERC CIP

Others

The SCADAfence Governance Portal is compared with self-reporting and sending auditing teams on-site. In comparison with those methods, the SCADAfence Governance Portal provides the following benefits: **Fully automated** – Doesn't require any manual labor in reporting. **Accurate** – An automated solution doesn't suffer from human errors and misunderstandings. **Up-to-date** – The reports are based on real time information coming from the remote sites. **No need to wait** for the next quarter or year to get results.

©Confidential and Proprietary Information of SCADAfence Ltd.

SCADAfence

About SCADAfence

SCADAfence is the global technology leader in OT & IoT cybersecurity. SCADAfence offers a full suite of industrial cybersecurity products that provides full coverage of large-scale networks, offering best-in-class network monitoring, asset discovery, governance, remote access, and IoT device security. A Gartner “Cool Vendor” in 2020, SCADAfence delivers proactive security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAfence enables organizations in critical infrastructure, manufacturing, and building management industries to operate securely, reliably, and efficiently. To learn more, go to SCADAfence.com

 ©Confidential and Proprietary Information of SCADAfence Ltd.