Logsign

# Logsign Next-Gen SIEM for ISO/IEC 27001

## How to Stay Compliant With ISO/IEC 27001

Datasheet

# Logsign Next-Gen SIEM for ISO/IEC 27001

ISO 27001 compliance requires the aggregation of event data from multiple systems and the security management of sensitive assets within an organization.

Logsign SIEM aggregates system, network and audit logs from various sources. These can be firewalls, routers, IDS/IPS, network devices, Windows, Linux/Unix, databases, VMware ESX, mail servers, web servers and more. Logsign SIEM allows you to quickly review the critical asset information required for ISO 27001 compliance, and increases awareness of potential security risks, vulnerabilities and threats in your organization.

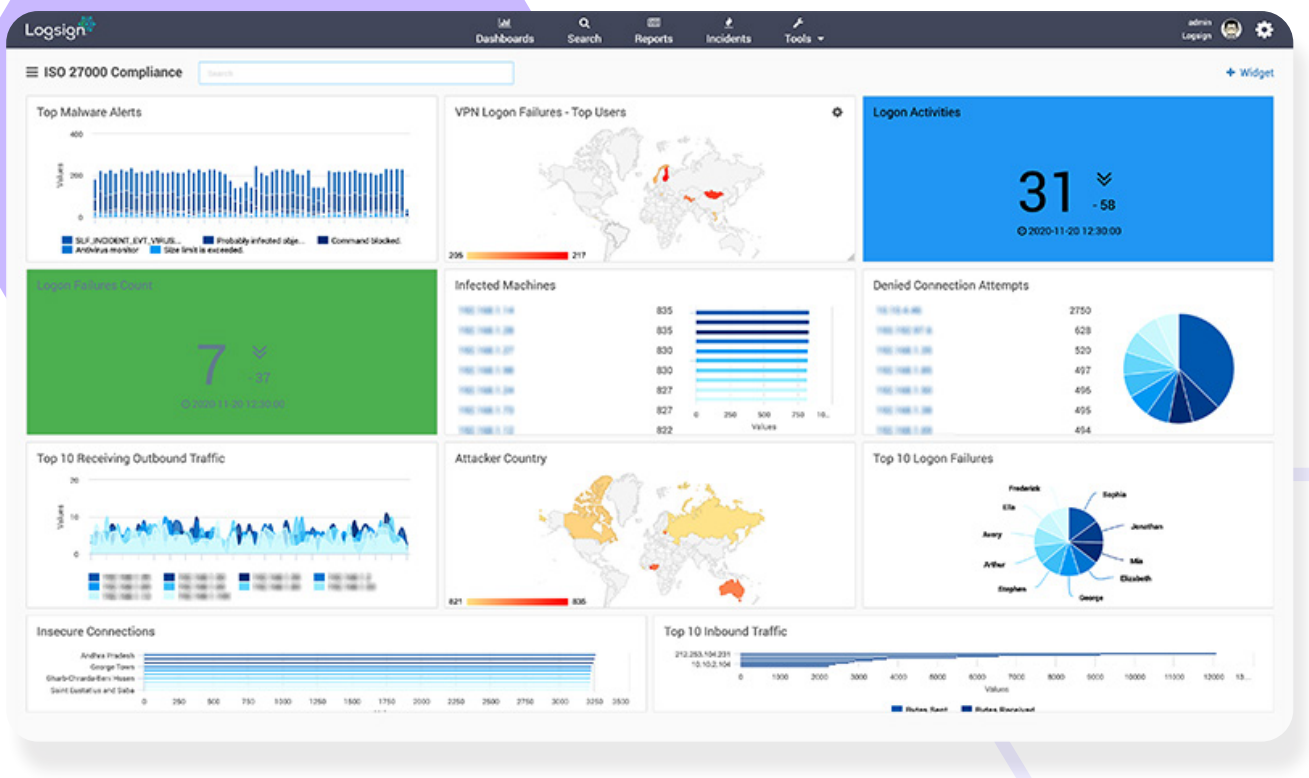
Logsign SIEM delivers essential security controls to achieve ISO 27001 compliance.Critical security information is visualized. Security incidents and threats are made visible in high-level reports and dashboards for real-time reviews. These include file integrity monitoring, collection of account management activities and audit logs. Continuous security monitoring quickly detects policy violations, malicious activities targeting sensitive assets and changes in critical files. Customization of report templates ensures that users can easily generate and distribute relevant reports in various formats (PDF, e-mail, etc.) for regulatory compliance.

## Highlights

Real-Time monitoring and reporting capabilities for PCI DSS Compliance.

Flexible and simple search and reporting capabilities to quickly answer any data request.

Predefined dashboards and reports.



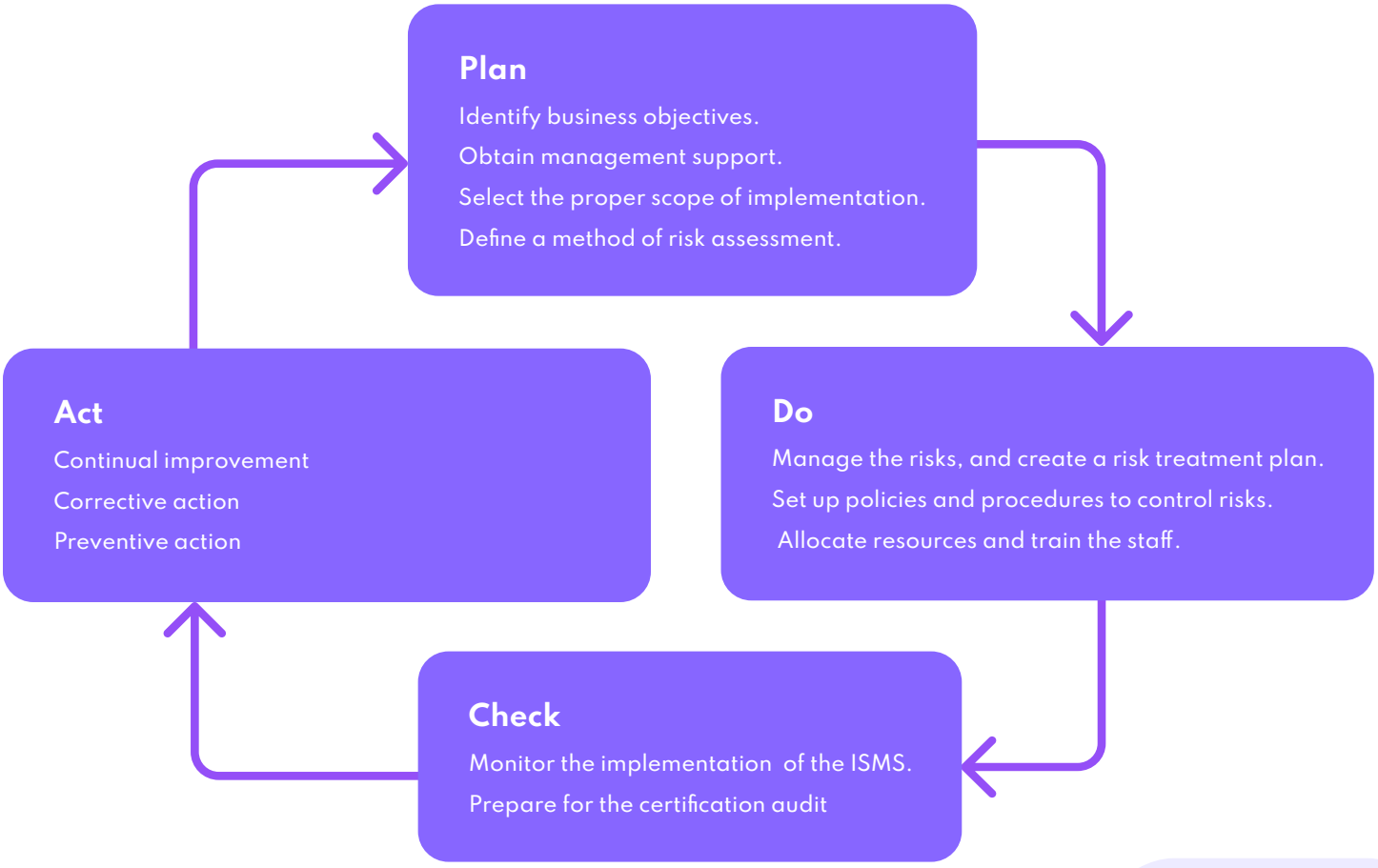

Logsign

# ISO 27001 (International Organization for Standardization)

ISO/IEC 27001 formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information risks (called 'information security risks' in the standard). The ISMS is an overarching management framework through which the organization identifies, analyzes and addresses its information risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts - an important aspect in such a dynamic field, and a key advantage of ISO27001's flexible risk-driven approach as compared to, say, PCI-DSS.

The standard covers organizations of all types (e.g. commercial enterprises, government agencies, non-profits)all sizes (from micro-businesses to huge multinationals), and all industries or markets (e.g. retail, banking, defense, healthcare, education and government). This is clearly a very wide range.

ISO 27001 is the management framework that follows the Four-Stage Process Cycle known as Plan-Do-Check-Act for information security controls. This aims to improve the Information Security Management System (ISMS) within the context of organization's overall business risks.



| ISO 27001 Compliance Requirements | Description | Logsign SIEM Solution |
|---|---|---|
| A.6.1.3 | Organization of Information Security | Logsign SIEM tracksspecific security tasks and stores log information related to security incidents and metrics. Logsign SIEM also tracks the alarm status and delegates it to someone if the current state changes. |
| A.8.3.1<br>A.8.3.3 | Human Resource Security | Logsign SIEM collects all account management events and tracks the access rights of all employees. Activities such as User login, denying, deleting or disabling are retained and reported by the platform.Logsign can also provide an alert if an account that should have been suspended suddenly becomes active. |
| A.10.1.2<br>A.10.3.1<br>A.10.3.2<br>A.10.4.1<br>A.10.5.1<br>A.10.6.1<br>A.10.9.3<br>A.10.10.1<br>A.10.10.2<br>A.10.10.3<br>A.10.10.5 | Communications and Operations Management | Logsign SIEM helps to evaluate information assets using the concepts of confidentially, integrity and availability. With real-time file integrity monitoring, modifications, deletions, permission changes, and additions to the file system can be made visible via reports and dashboards. Logsign SIEM monitors system operations and detects unauthorized changes to the system. Information on disk volume status, CPU utilization and other hardware performance, service initiations andinterruptions can be monitored. Accordingly, notifications and real-time alerts for abnormal changes and configurations will be triggered. Logsign SIEM collects logs from various sources, such as network devices, hosts, firewalls,IDS/IPS systems, endpoint security systems and other security devices. These are made visible in reports and dashboards but are also actionable with alarms against malware, virus and other security attacks. E-mail and audit trail logs are also collected, analyzed and reported to meet confidentially, integrity and availability requirements for all information assets. |
| A.11.2.1<br>A.11.5.1<br>A.11.5.4<br>A.11.6.1 | Access Control | Logsign SIEM can monitor the entire account management process and account usage activity, including user account deletion/creation, privileged changes, access escalation, hosts, password changes and VPN usage. File integrity monitoring provides reviews on file permission changes, detected access and use of utilities. Whenever unauthorized activity is detected, reports and alerts ensure awareness about these abnormal activities. |
| A.12.4.2<br>A.12.4.3<br>A.12.5.1<br>A.12.6.1 | Information System Acquisition, Development and Maintenance | Logsign SIEM is fully deployed with file integrity monitoring. This helps to review information including access, modifications, permission changes to the file system and configuration and changes to the performance of operational software. The visualisation of configuration changes can be used for analysis Wand reporting. Logsign SIEM can also monitor vulnerabilities in the IT infrastructure and report on them as metrics for patching systems. It can also monitor system uptime metrics. |
| A.13.1.1<br>A.13.1.2<br>A.13.2.1<br>A.13.2.2<br>A.13.2.3 | Information Security Incident Management | Logsign SIEM monitors vulnerabilities in the IT infrastructure and reports on them as metrics for patching systems. It can also monitor system uptime metrics.Logsign SIEM enables security event management with reports and alarms to review vulnerabilities in the IT architecture and provides a complete record of incident classification. |
| A.14.1.2 | Business Continuity Management | Logsign SIEM collects, classifies, normalizes and analyzes the logs and creates reports and dashboards to review events in real-time. When problems are detected, Logsign SIEM takes action, monitors and reports the risk, creates an alarm in real-time, and sends notification to the administrator |
| A.15.1.3<br>A.15.3.2 | Compliance | The ability of Logsign SIEM to analyzeng and report can be used for monitoring configuration changes. Automated auditing of data integrity, availability and confidentiality facilitate the regulatory compliance of the organization with security policies. |

## About Us

Logsign was established in 2010 to enable cyber security practitioners to work more efficiently with smart, clutter-free and next-generation softwares. Securing the IT systems and managing cyber security operations should not be so complex, time consuming and over-priced. This is why we developed our smart and simple-to-use SIEM and SOAR softwares considering the market's current and future needs. Automation starts the new era in cybersecurity. We believe with this era, automation handles the manual workload of humans upto 98%. Thus, efficiency in cybersecurity operations is not a dream anymore. SOAR software is in the heart of operations enhancing security teams work in a smart, collaborative and effective environment. You can't protect before you see and detect. Collecting any data, visualizing and turning into actionable intelligence are possible via our infinitely scalable and cluster SIEM. With 10 years of experience, Logsign is a sincere team player for all internal & external parties, trusted by more than 500 enterprises, ministries and state agencies.

www.logsign.com

support.logsign.net

0 850 660 0 850