LOGSIGN FOR ISO 27001 COMPLIANCE

AUTOMATE LOG MANAGEMENT FOR AND STAY COMPLIANCE WITH ISO 27001

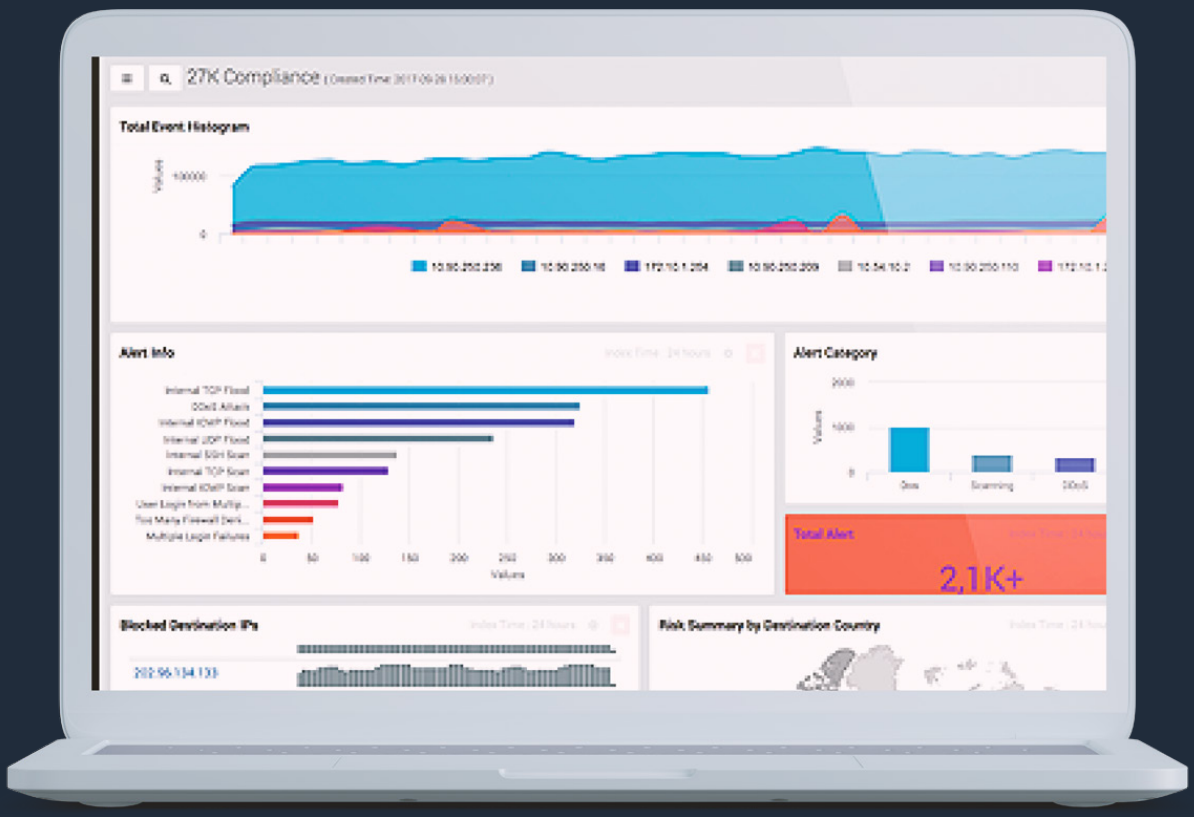
ISO 27001 compliance requires the aggregation of event data from multiple systems and the security management of sensitive assets within an organization.

Logsign 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 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 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, reporting and alerting of ISO 27001 compliance.
- Flexible and faster searching and reporting capabilities to quickly answer any ISO 27001 compliance data request.
- Pre-built dashboards quickly identify and prioritize areas of ISO 27001.
- Collect, Archive and Recover.
- 360 degree visibility of IT infrastructure.



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 Solutiovn
A.6.1.3	Organization of Information Security	Logsign tracksspecific security tasks and stores log information related to security incidents and metrics. Logsign also tracks the alarm status and delegates it to someone if the current state changes.
A.8.3.1 A.8.3.3	Human Resource Security	Logsign 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 A.10.3.1 A.10.3.2 A.10.4.1 A.10.5.1 A.10.6.1 A.10.9.3 A.10.10.1 A.10.10.2 A.10.10.3 A.10.10.5	Communications and Operations Management	Logsign 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 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 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 A.11.5.1 A.11.5.4 A.11.6.1	Access Control	Logsign 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 A.12.4.3 A.12.5.1 A.12.6.1	Information System Acquisition, Development and Maintenance	Logsign 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 and reporting.Logsign 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 A.13.1.2 A.13.2.1 A.13.2.2 A.13.2.3	Information Security Incident Management	Logsign monitors vulnerabilities in the IT infrastructure and reports on them as metrics for patching systems. It can also monitor system uptime metrics. Logsign 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 collects, classifies, normalizes and analyzes the logs and creates reports and dashboards to review events in real-time. When problems are detected, Logsign takes action, monitors and reports the risk, creates an alarm in real-time, and sends notification to the administrator
A.15.1.3 A.15.3.2	Compliance	The ability of Logsign 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.

Logsign is a Security Information and Event Management (SIEM) solution which provides security analyses and compliance to regulations in one platform. Founded in 2010, Logsign believes that cyber security is a teamwork and that security products have to be much smarter. With this conviction, it focused its endeavors on Security Intelligence and SOC solutions. It actively provides services for more than 500 medium and large scale firms and governmental agencies. It is working to be an irreplaceable team-mate for all of its stakeholders in the field of cyber security, to raise its customers' security awareness to the maximum and to reinforce their position concerning security. It also proved its competence in the field of technology as a cyber security software producer, landing among Deloitte Technology EMEA Fast 500 in 2017 for the second time.