ManageEngine
Log360

How to comply with

ISO 27001:2022

SECURITY CONTROLS USING SIEM

Anupama. A

Table of contents

Chapters

ISO 27001 is a cybersecurity certification and framework that helps companies implement an information security management system (ISMS) tailored to meet their security and business requirements.

An ISMS helps organizations determine the controls they need for the safety of their data, and thus helps structure an organization's approach to information security.

The latest update of this framework was published on October 25, 2022, and observably, there are some major changes. Auditors and organizations alike were eagerly awaiting this updated and consolidated version of the standard, after multiple corrigenda were added in 2014, 2015, and 2017. Different organizations were adopting different versions of this standard, and this caused problems for both themselves and auditors.

In this e-book, you will get a detailed overview of ISO 27001 and its certification process. You will also learn about the security technologies you can implement to adhere to the controls mentioned in ISO 27001.

Chapter 1

Introducing ISO 27001

The ISO 27000 family of standards consists of best practices and controls organizations can use to implement an information security management system (ISMS) and the CIA (confidentiality, integrity, and availability) triad to protect their data. The primary goal of the ISO 27001 security standard is to help organizations set up an ISMS that best fits their risk profile and requirements.[1]

Why choose ISO 27001?

ISO 27001 is a widely recognized regulatory standard. Apart from the stellar reputation of being ISO 27001 certified, complying with the standard helps organizations:

1. Maintain better cybersecurity posture.
2. Comply with other regulatory standards.
3. Mitigate the risk of cyberthreats.
4. Stand out amongst competitors.

What is ISO 27001?

ISO 27001 is a cybersecurity standard and framework which helps organizations put an ISMS in place. Since it is a risk-based approach, it helps organizations gauge their security posture. Organizations are first required to conduct a cybersecurity risk assessment and identify their areas of risk. Then, they need to implement security controls and measures to put in place an ISMS that helps them fulfill their risk requirements.

How did ISO 27001 come to be?

The original version of ISO 27001 was known as BS 7799, and was drafted by the United Kingdom's Department of Trade and Industry. It was published by the British Standards Institution in two parts, the first in 1995 and the second in 1999. The first part became **ISO/EC 17799** and was called Information Technology: Code of Practice for Information Security Management. The second part, called Information Security Management System, was adopted as part of risk management and assessment in the ISO 27000 series. It is now called ISO 27001.

The latest version of ISO 27001 was published in 2013 with minor updates implemented in 2014, 2015, and 2017.

How is ISO 27001 structured?

ISO 27001 is divided into two parts:

Part one:

This consists of 12 sections. These sections include the introduction, scope, and 10 clauses:

a. Introduction
b. Scope
c. Normative details
d. Terms and definitions
e. Context of the organization
f. Leadership
g. Planning
h. Support
i. Operation
j. Performance evaluation
k. Improvement
l. Reference control objectives and controls

Part two:

Annexure A: The second part of ISO 27001 is Annexure A, which consists of 93 controls, further divided into five sections. It is a continuation of part one and picks up after clause 10.

Is it a mandatory compliance standard?

ISO 27001 is not a compliance mandate. It helps organizations focus on their unique security requirements and implement an ISMS. However, organizations that aim to obtain an ISO 27001 certification must comply with the standard.

How are ISO 27001 and 27002 different?

While ISO 27001 is a framework for which organizations can obtain a certification, ISO 27002 is a best practice guide that provides recommendations to implement the ISO 27001 controls in Annexure A. Organizations can choose which best practices to implement from ISO 27002, as there is no certification provided.

In the following chapter, we will look into what an ISMS is, how organizations stand to benefit by implementing it, and how they can go about implementing it.

Chapter 2

Implementing an information security management system (ISMS)

An ISMS helps organizations determine the controls they need for the safety of their data, and thus helps define an organization's approach to information security. [2]

Why do companies need an ISMS?

An ISMS enables organizations to implement the CIA triad of data protection. The CIA triad consists of:

A

Confidentiality

Organizations must take measures to protect the privacy of their data, like ensuring authorized and restricted access.

B

Integrity

Organizations must sustain the authenticity and reliability of data, and make sure it is error-free to facilitate data integrity.

C

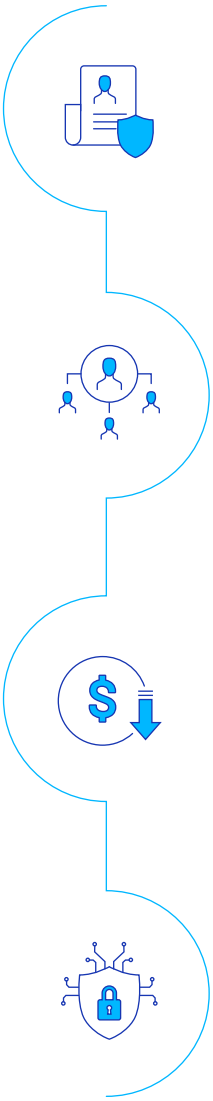
Availability

Organizations must ensure the availability of data at any time. This means ensuring all systems and operations that deal with data function smoothly, and taking steps to eliminate redundant servers and improve the speed of updates.

Implementing all three parts of the CIA triad significantly increases cyber resilience and improves the capability of organizations to handle threats.

Benefits of an ISMS

Apart from being compliant with ISO 27001, having an ISMS in place provides several advantages to an organization:



Safeguarding privileged information

With the primary objective of protecting the confidentiality, integrity, and availability of information, an ISMS works to safeguard the various information assets in an organization.

Centralized management system

An ISMS ensures that all data is stored, secured, and managed in a centralized fashion. This holistic approach leads to an increase in security and contributes to the organization's overall growth.

Reduction of security costs

Since an ISMS is implemented based on each organization's risk assessment, it can help avoid costs incurred due to experimenting with various security solutions. Taking a centralized approach leads to a reduction in overall costs as well.

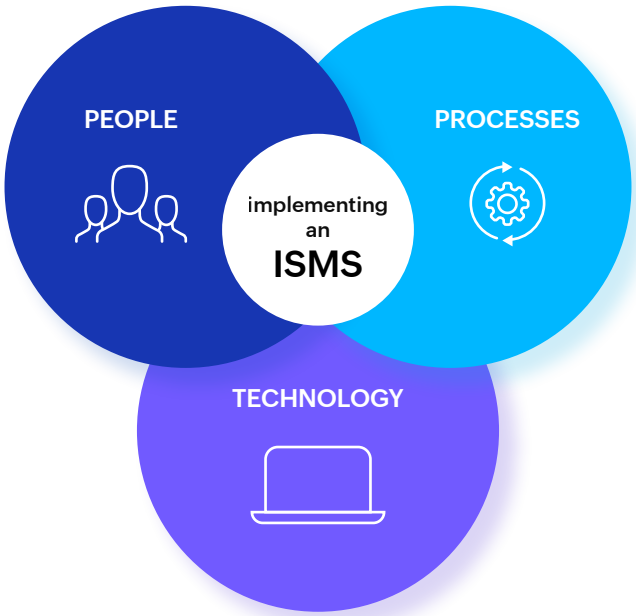
Increase in cyber resilience

An ISO-27001-compliant ISMS requires organizations to change their security measures constantly and evolve with the threat landscape. This leads to an overall increase in cyber resilience.

Implementing an ISMS

ISO 27001 recommends the plan-do-check-act, or the PDCA method, for implementing an ISMS. The PDCA method is actively followed in all ISO standards and appears in part one of the ISO 27001 standard. PDCA is a cyclical method wherein companies have to check their progress continuously. It aligns with ISO 27001's continual improvement formula and helps companies consistently evaluate themselves, instead of relying solely on audits.

This formula makes implementing an ISMS a company-wide exercise, which includes the intersection of important people, processes, and technology, as illustrated in the image below. Let's take a brief look at what these entail.



People

There are several stakeholders involved in implementing an ISMS. Clause 4.2 in the standard talks about the needs and expectations of "interested parties" that the organization must determine while implementing an ISMS.

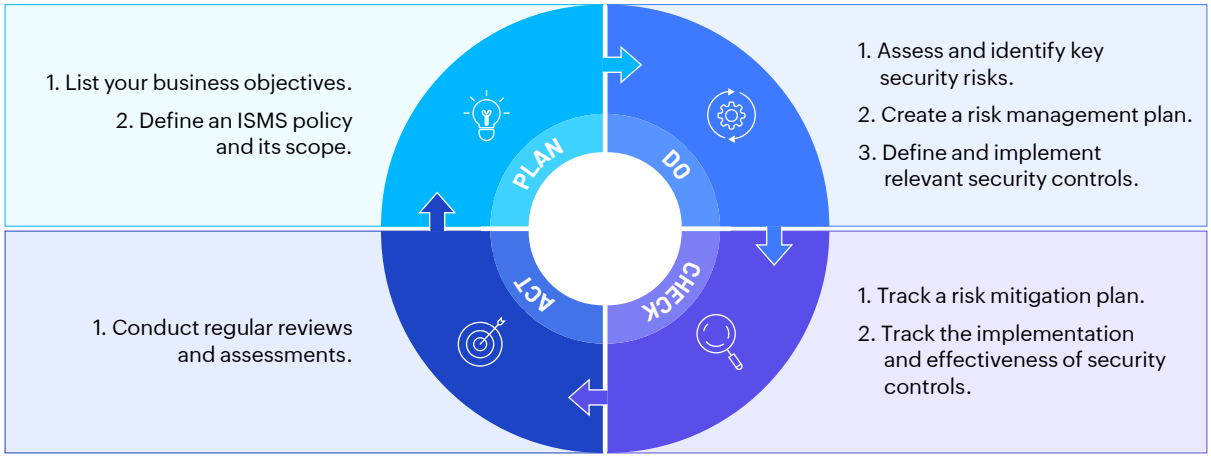
> **Clause 4.2:** [3]
> The organisation shall determine:
> a) interested parties that are relevant to the information security management system
> b) the requirements of these interested parties
> c) which of these requirements will be addressed through the information security management system

Interested parties could denote any stakeholder or entity that could be affected by the business continuity or information security controls in an organization. This could include:

- Employees
- Government or accreditation agencies
- Clients
- Top management
- Department heads

Processes

Here's where the PDCA fits in. Implementing an ISMS can be defined through the following steps, as illustrated in the image below:



Necessary changes are implemented based on the assessment. This is then followed in a cyclical manner to ensure continuous improvement and an up-to-date risk posture for the organization.

Technology

Implementing an ISMS can be a daunting task for organizations. With the new update introducing notable changes, organizations must invest in automated technologies that can easily help them comply with the security controls listed in the standard.

Some of these technologies include:

- Data security platforms.
- Compliance management solutions.
- Security information and event management (SIEM) solutions.

In this chapter, we've explored how to implement an ISMS, and the various people, processes, and technologies involved in its implementation. The latest standard, published in 2022, carries significant changes that affect these factors. The following chapter explores these changes in detail and gives organizations the gist of all they need to know about getting ISO 27001:2022 certified.

Chapter 3

Understanding the major changes in ISO 27001:2022

After the last corrigenda in 2017, the latest version of ISO 27001, released in October 2022, was highly anticipated. And it does not disappoint.

Though there are several structural updates, the 2022 version notably focuses on practical, result-based outcomes for organizations. Deviating from the usual compliance checklist method of implementing an ISMS, this new version emphasizes a more evidence-based method for security controls.[4]

Overview of major changes

Some of the major changes in ISO 27001 are structural changes made to the security controls listed in part two and some minor edits made to the clauses in part one.

While the edits made to part two signify a change in outlook towards implementing an ISMS, the changes made to part one indicate a shift in perspective when it comes to cybersecurity.

Clause-wise changes made in part one

Clause/ subclause	Title	Subclause in ISO 27001:2013	Change in ISO 27001:2022
Clause 4	**Context of the organization**		
4.2	**Understanding the needs and expectations of interested parties**	The organization shall determine: a. interested parties that are relevant to the information security management system; and b. the requirements of these interested parties relevant to information security.	One new sub-item has been added: c. Which of these requirements will be addressed through the information security management system.
4.4	**Information security management system**	The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of the international standard.	The organization shall establish, implement, maintain and continually improve an information security management system,

			including the processes needed and their interactions, in accordance with the requirements of this International Standard.
Clause 6	**Planning**		
6.2	**Information security objectives and planning to achieve them**	The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall: a. be consistent with the information security policy b. be measurable (if practicable) c. take into account applicable information, security requirements, and results from risk assessment and risk treatment d. be communicated; and e. be updated as appropriate. The organization shall retain documented information on the information security objectives. When planning how to achieve information security objectives, the organization shall determine: f. what will be done g. what resources will be required h. who will be responsible i.when it will be completed j. how the results will be evaluated.	Two new sub-items have been added: (The information security objectives shall:) d. be monitored g. be available on documented information
6.3	**Planning of Changes**	This sub-clause was newly added and is not present in the 2013 version.	Any change made to ISMS must be carried out in a planned manner.

Clause 7	Support		
7.4	**Communication**	The organization shall determine the need for internal and external communications relevant to the information security management system including: a. on what to communicate b. when to communicate c. with whom to communicate d. who shall communicate and e. the process by which communication shall be effected.	One new sub-item has been added: d. how to communicate
Clause 8	**Operation**		
8.1	**Operational planning and control**	The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also	The organization shall ensure that externally provided processes, products or services that are relevant to the ISMS are controlled.
Clause 9	**Performance evaluation**		
9.1	**Monitoring, measurement, analysis and evaluation**	The organization shall evaluate the information security performance and the effectiveness of the ISMS. The organization shall determine: a. what needs to be monitored and measured, including information security processes and controls b. the methods for monitoring, measurement, analysis and evaluation, as applicable to ensure valid results. c. when the monitoring and measuring shall be performed d. who shall monitor and measure	• Documented information shall be available as evidence of the results. • Organizations shall evaluate the information security performance and the effectiveness of the ISMS.

		e. when the results from monitoring and measurement shall be analysed and evaluated and f. who shall analyse these results The organization shall retain appropriate documented information as evidence of monitoring and measurement results.	

Structural changes made to part two (security controls) [5]

Consolidation and addition of controls

An ISO-27001-compliant ISMS requires organizations to change their security measures constantly and evolve with the threat landscape. This leads to an overall increase in cyber resilience.

- Threat intelligence
- Information security for use of cloud services
- ICT readiness for business continuity
- Physical security monitoring
- Monitoring activities
- Web filtering
- Secure coding
- Configuration management
- Information deletion
- Data masking
- Data leakage prevention

Decrease in the number of sections

Previously, all 114 control items were divided into 14 domains. Each of the 14 domains dealt with a different function in an organization. The current 93 controls have been divided into four groups or themes now, and function-based division has been eliminated. These four themes include:

- Organizational controls
- People controls
- Physical controls
- Technological controls

Addition of a new subclause

Clause 6.3—Planning of Changes—is newly introduced in the latest version. We will explore this in detail in the section titled Clause-wise changes made in part one.

Attributes

Each control in the new version comes with attributes. These attributes will help organizations customize and pick controls that best suit their cybersecurity needs. There are five such attributes used to categorize the 93 controls:

- Control types
- Information security properties
- Cybersecurity concepts
- Operational capabilities
- Security domain

Some of the attributes have been borrowed from other frameworks. For example, under cybersecurity concepts, the framework enlists the Identify-Detect-Protect-Recover-Respond cycle found in the NIST framework. Attributes also enable organizations to clearly understand which processes, people, and technology are essential and involved in the implementation and maintenance of an ISMS.

Language and content change

There has been a notable change in the language used in ISO 27001:2022, starting with the title of the ISO 27001 standard. Earlier known as the Information technology — Security techniques — Information security management systems — Requirements, the latest 2022 version contains Information security, **cybersecurity and privacy protection** — Information security management systems — Requirements.

The addition of the word cybersecurity is an indicator of the dire need for organizations to secure their systems in the current threat landscape. ISO 27001 aims to address this through the implementation of the various security controls listed in the document to create an ISMS.

In several places, the language is also more active in nature when compared to the 2013 version. The overall approach outlined in the standard is practical and result- or evidence-based as opposed to the checklist method followed earlier.

Emphasis on cloud security

The rising adoption of cloud technologies has prompted organizations to increase security measures pertaining to the cloud, and this is reflected in ISO 27001:2022 as well. One of the 11 new controls added to the list is information security for the use of cloud services, and it extensively explores how organizations must use cloud services. Implementing this control will help strengthen the cloud security measures in an organization.

All the changes collectively point to a new process-based approach adopted by the standard, similar to the ISO 9000 standard.

What the new changes signify

The ISO 27001 framework has been constantly criticized for being a management standard as opposed to a cybersecurity standard. Its risk-based management approach depends on the method defined by each organization to identify risk and address it using the security controls listed in the standard.[6] The earlier version focuses on the organization's ability to identify risk correctly without going deeper into the people or processes involved in making that happen. The ISO 27001:2022 version is more process-oriented, in line with the ISO 9000 approach, and focuses on enabling organizations to recognize and continually improve the processes they have in place.

What all certified organizations must know

ISO 27001 certified organizations have a transition time of three years from the date of publication of the new version of the standard to start making the above-mentioned changes. The 2022 version of the standard was published on October 25, 2022.

What all organizations that want to be ISO 27001 certified must know

There haven't been any changes to the ISO 27001 certification process, which is outlined and explained in detail in the coming chapter.

Chapter 4

Complying with ISO 27001 security controls using SIEM

To obtain the coveted ISO 27001 certification, an organization will have to show that it has successfully implemented an ISMS and has taken the necessary steps to address risks.

Different stages in an ISO certification process

The audit for an **ISO 27001 certification** takes place in two stages:

Stage 1

This is when an auditor does a review of the documented ISMS and assesses whether it meets the requirements of the standard. Organizations need to produce a Statement of Applicability, which is a vital requirement for certification. It consists of the chosen controls from the list of 93 controls in Annexure A, the implementation procedure of each of them, and the list of omitted controls and why they have been omitted. This is mostly a desktop exercise, and there is minimal interaction with the people tasked with overseeing the implementation of the ISMS.

Stage 2

The organization is audited to see if the processes it has in place are as documented in the ISMS. The auditors also interview those responsible for operations, look into the evidence for all the documentation, and review the controls implemented to address risk. Usually three months' worth of proof is required.

Once acquired, an ISO 27001 certification is valid for three years, after which a re-certification assessment is conducted. After certification, organizations can expect surveillance visits at least once every year to ensure they are evolving and adding the latest security measures to stay vigilant and up to date.

Complying with ISO 27001's new security controls using SIEM

Implementing an ISO-27001-compliant ISMS means implementing strict access control measures to upkeep the confidentiality, integrity, and availability of sensitive data. Organizations need to record and regularly review event logs, protect them from unauthorized access, and ensure secure logon procedures are followed.[7]

Here's how a SIEM solution can help with the 11 new controls that were recently added to ISO 27001. The numbers and titles mentioned below are similar to the format followed in the ISO 27001:2022 document.

5.7 Threat intelligence

What the control is about: Organizations are required to gather threat intelligence from various sources and use this information to implement preventive controls in their systems for incident management, security operations, and supplier or partner relations security purposes.

How a SIEM solution can help you with this: SIEM solutions come equipped with a threat intelligence feature that can help organizations stay up to date with the latest threats. SIEM tools like ManageEngine Log360 gather intelligence from STIX and TAXII feeds and integrate with Webroot and BrightCloud threat intelligence services. This helps the solution provide real-time alerts when network activity involving blacklisted IPs and URLs is detected.

5.23 Information security for use of cloud services[8]

What the control is about: Organizations need to define a process to monitor cloud usage, including the purchase, use, and management of cloud services.

How a SIEM solution can help you with this: Organizations must have the ability to monitor the cloud and detect cloud-based attacks. With organizations moving to multi-cloud infrastructures, it is vital to monitor activities across multiple cloud providers. Log360 comes equipped with a cloud security monitoring component, which enables companies to monitor Amazon Web Services, Google Cloud Platform, and Microsoft Azure, and generate reports for network activity.

5.30 ICT readiness for business continuity

What the control is about: This control refers to information and communication technology (ICT) readiness planning to ensure the organization is prepared with backups and a data recovery plan in case of any disruptions to systems.

A data recovery manager like ManageEngine's Recovery Manager Plus can help organizations back up their Exchange online, on-premises, and Google Workspace mailboxes by scanning data snapshots and storing them in air gaps.

7.4 Physical security monitoring

What the control is about: Organizations must set up appropriate physical security measures to ensure sensitive areas are appropriately protected through security cameras or guards, and come up with an incident management plan for physical security incidents.

How a SIEM solution can help you with this: IoT has paved the way for new dimensions in cybersecurity. Security cameras set up for physical security monitoring produce network video recorder and digital video recorder system logs. These consist of power on or off logs, and restart, account access, or hard disk error logs. These can be analyzed and monitored to detect suspicious activity as well.

8.9 Configuration management

What the control is about: This control requires organizations to have configurations or parameters in place to manage and monitor all the hardware and software components that are part of a network. This is a part of asset management and needs to be documented and presented during an audit.

How a SIEM solution can help you with this: A SIEM tool can help organizations continuously monitor their networks and keep an eye on their network devices and endpoints. It collects and analyzes logs generated from these devices and presents them as reports. This makes it easier for security analysts to monitor these devices and detect any unwarranted changes to the network.

8.10 Information deletion

What the control is about: Organizations generate a lot of data and need to set up a safe process to delete data in a secure fashion periodically.

How a SIEM solution can help you with this: A SIEM solution like Log360 comes equipped with a file storage analysis and data visibility module that helps organizations identify and erase redundant data in a secure and cost-efficient manner.

8.11 Data masking

What the control is about: As the name suggests, data masking refers to the process of curbing access to sensitive data and ensuring availability to authorized personnel. This is especially applicable to personal data due to the various privacy regulations placed on it.

How a SIEM solution can help you with this: An IT administrator or security analyst can use a SIEM solution to track who accesses data that needs to be masked or secured, and receive alerts when this happens.

8.12 Data leakage prevention

What the control is about: Along with setting up processes that determine how sensitive a file is or the amount of risk it possesses, organizations must also set up systems to monitor avenues through which there is high risk of data leakage. In case a data leak or a similar security incident occurs, it must be resolved in a timely manner.

How a SIEM solution can help you with this: In this post-lockdown world, which is busy transitioning from a fully remote to a hybrid work environment, remote systems are highly vulnerable. A SIEM solution can help monitor remote systems by keeping an eye out for VPN or cloud-based attacks. Analysts can generate file activity and file integrity monitoring reports to regularly scan and analyze abnormalities in the network. A cloud access security broker or CASB-enabled SIEM solution can help keep an eye on suspicious cloud app usage and spot activities like malicious file downloads.

8.16 Monitoring activities

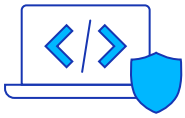
What the control is about: This requirement states that all organizations should monitor and update all event logs, including those from security applications, to keep an eye on all network traffic and monitor access to confidential information. Organizations must also have an incident response plan in place in case such a security incident occurs.

How a SIEM solution can help you with this: A SIEM tool with SOAR and incident management capabilities is the perfect solution for all organizations. ManageEngine's SIEM solution, Log360, can help organizations keep an eye on network activity with over 1,000 predefined reports that help security analysts spot suspicious security incidents. It comes equipped with MITRE-ATT&CK®-based reports, which help them create alert profiles for the latest cyberattacks.

8.23 Web filtering

What the control is about: Organizations must ensure there are measures in place to stop users from visiting malicious websites and to detect the execution of malicious code.

How a SIEM solution can help you with this: SIEM solutions come equipped with threat intelligence feeds that have a list of blacklisted IPs from around the world and prebuilt reports that help detect malicious code executions. Security teams can also create custom reports and alert profiles for suspicious cloud activity and set up cloud access policies to prevent file tampering and protect data. A SIEM solution integrates with firewalls, which organizations can use to set up policies that can block connection requests from malicious IPs, which can be obtained from integration with threat intelligence feeds like STIX and TAXII.



8.28 Secure coding

What the control is about: Organizations must establish secure coding best practices applicable during and after coding. They must also ensure these are regularly followed by all coders. Source codes must be protected with limited access and proper authorization protocols. Any violation or unauthorized attempts to access this must be detected and curbed.

How a SIEM solution can help you with this: SIEM solutions can help organizations detect unauthorized access and execute a set of protocols to nip this in the bud using automated workflows.

To learn more about how a SIEM solution like ManageEngine Log360 can help you comply with these 11 new controls in ISO 27001:2022, you can sign up for a free, personalized demo with our product experts here.

About ManageEngine Log360

ManageEngine Log360, a SIEM solution with extensive log management capabilities, automates the collection of logs in terabytes. It ensures that collected logs are securely archived for analysis through file integrity monitoring and helps organizations maintain access control measures through its out-of-the-box security reports. These help keep track of successful and unsuccessful logon attempts, user activity, and authorization access to critical devices and applications. Log360 also helps keep track of changes made to user, domain, and audit policies that organizations can use to make sure reliable logon procedures are in place. These changes can be monitored, analyzed, and generated as real-time, audit-ready reports that can contribute significantly to compliance procedures.

To learn more about how Log360 can help you comply with ISO 27001, sign up for a free, 45-day trial to evaluate it yourself, or request a personalized demo with our product experts.

About the author

Anupama is a product marketing associate at ManageEngine, the enterprise IT management division of Zoho Corporation. In her current role, she keeps track of the latest trends in the cybersecurity space, especially those related to SIEM. A keen writer, she contributes to organizational cybersecurity awareness through her research-led insights.

References

1. A, Anupama. “Getting Started with ISO 27001? Here's What You Need to Know.” ManageEngine Log360 Expert Talks . ManageEngine, May 26, 2022. https://www.manageengine.com/log-management/cyber-security/iso-27001-certification-what-you-need-to-get-started.html.

2. “ISO/IEC 27001:2013 Information Technology-Security Techniques-Information Security Management Systems-Requirements.” BSI . Accessed January 23, 2023.

3. Clark, Quentin. “ISO 27001 - Understanding & Communicating with Stakeholders.” StandardFusion, November 8, 2022. https://www.standardfusion.com/blog/iso-27001-understanding-communicating-with-stakeholders/.

4. Sepulveda, Sebastian. “ISO 27001:2022 Everything You Need to Know about the Main Changes.” StandardFusion, December 20, 2022. https://www.standardfusion.com/blog/iso-27001-changes-2022/.

5. “2022 Update ISO 27001 Information Security Management.” 2022 update ISO 27001 Information Security Management | India. Accessed January 23, 2023. https://www.bsigroup.com/en-IN/ISOIEC-27001-Information-Security/ISOIEC-27001-revision/.

6.Jansen, Dr. Henk Jan. “Why ISO 27001 Is Not Enough.” LinkedIn. Accessed January 23, 2023. https://www.linkedin.com/pulse/why-iso-27001-enough-prof-dr-ir-henk-jan-jansen.

7. Kosutic, Dejan. “What Are the 11 New Security Controls in ISO 27001:2022?” 27001Academy, January 20, 2023. https://advisera.com/27001academy/explanation-of-11-new-iso-27001-2022-controls/.

8.“ISO 27002:2022 – Control 5.23 – Information Security for Use of Cloud Services.” ISMS.online. Accessed January 23, 2023. https://www.isms.online/iso-27002/control-5-23-information-security-for-use-of-cloud-services/.